

TRANSACTIONS OF
THE ROYAL SOCIETY
OF CANADA

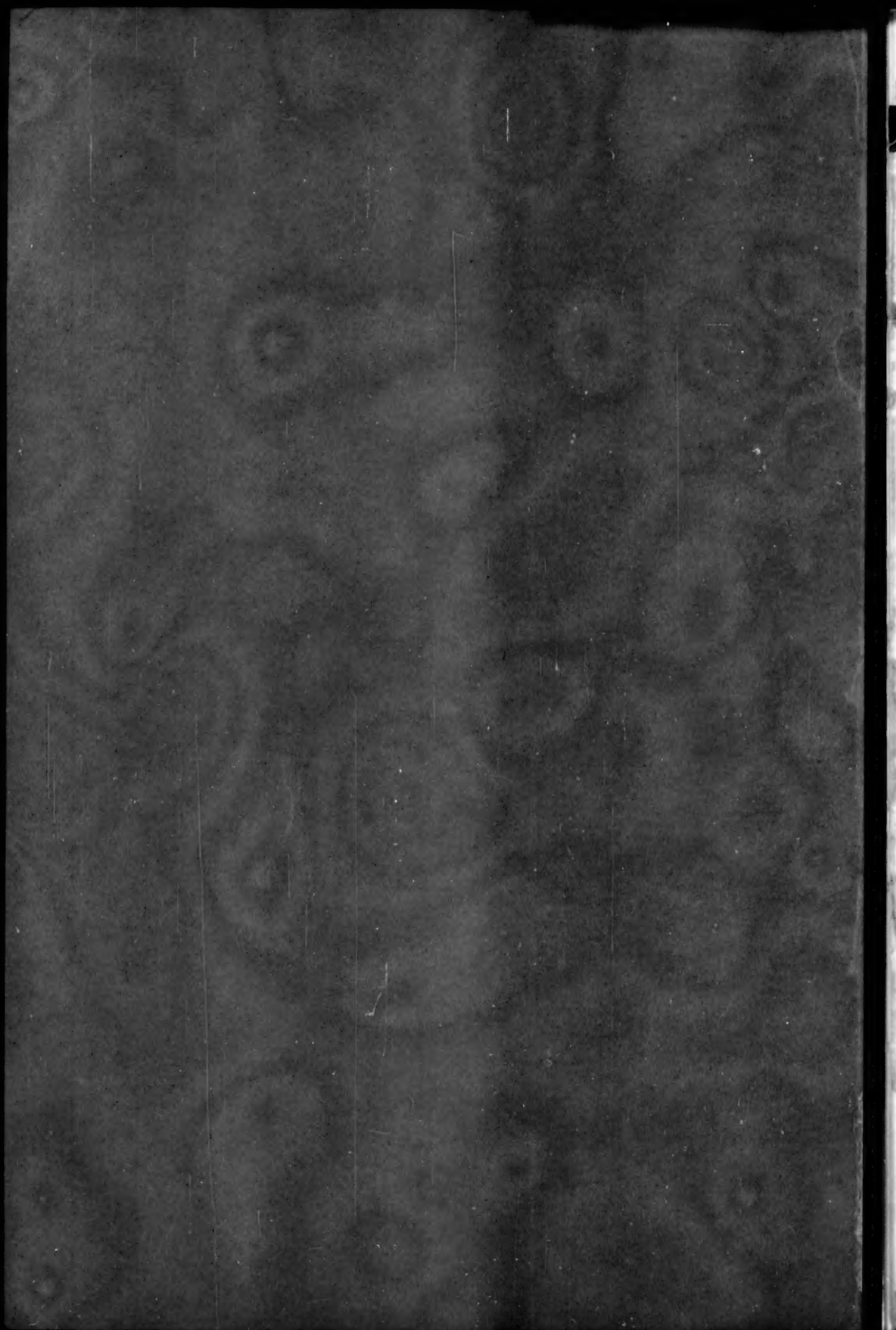
SECTION III
CHEMICAL, MATHEMATICAL,
AND
PHYSICAL SCIENCES



THIRD SERIES—VOLUME XLVIII—SECTION III

JUNE, 1954

OTTAWA
THE ROYAL SOCIETY OF CANADA
1954



TRANSACTIONS OF
THE ROYAL SOCIETY
OF CANADA

SECTION III
CHEMICAL, MATHEMATICAL,
AND
PHYSICAL SCIENCES

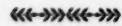


THIRD SERIES—VOLUME XLVIII—SECTION III

JUNE, 1954

OTTAWA
THE ROYAL SOCIETY OF CANADA
1954

CONTENTS



<i>Upper and Lower Estimates for the Area of a Triangle.</i> By S. BEATTY, F.R.S.C.	1
<i>Tangents to Ovals with Two Equichordal Points.</i> By LLOYD DULMAGE	7
<i>Coordinates in Geometry, I.</i> By K. D. FRYER and ISRAEL HALPERIN, F.R.S.C.	11
<i>An Inequality of Steinitz and the Limits of Riemann Sums.</i> By ISRAEL HALPERIN, F.R.S.C. and NORMAN MILLER	27
<i>On an Array of Aitkin.</i> By LEO MOSER and MAX WYMAN, F.R.S.C.	31
<i>On Ordered, Finitely Generated, Solvable Groups.</i> By RIMHAK REE . .	39
<i>Dually Differentiable Points on Plane Arcs.</i> By PETER SCHERK, F.R.S.C.	43
<i>Elementary Points on Plane Arcs.</i> By PETER SCHERK, F.R.S.C. . .	49

Upper and Lower Estimates for the Area of a Triangle

S. BEATTY, F.R.S.C.

1. Introduction. In a plane triangle ABC , let a, b, c denote the sides, Δ the area, R and r the circumradius and inradius respectively, and s, H , and K the symmetric functions $\frac{1}{2}(a+b+c)$, $\frac{1}{2}(a^2+b^2+c^2)$, and $(ab+bc+ca)$ respectively. Gerretsen (1) has given upper and lower estimates for Δ based on inequalities which become

$$(1) \quad \frac{(K-H)}{2} > \Delta\sqrt{3} > \frac{(K-H)}{2} - (2H-K)$$

when $4Rr + r^2$ is replaced by its value in terms of the sides, namely $\frac{1}{4}(K-H)$. The first of these inequalities was originally given by Weizenböck (2) and subsequently discussed by Finsler and Hadwiger (3).

The present paper presents the inequalities

$$(2) \quad \frac{(K-H)^2}{12} > \Delta^2 > \frac{(K-H)^2}{12} - \frac{(K-H)(2H-K)}{6}.$$

The first inequality in (2) amounts to the same as the first in (1) and hence needs no proof. The second inequality in (2) is an improvement on the second in (1), since this latter may be written in the form

$$\Delta\sqrt{3} \frac{(K-H)}{6} > \frac{(K-H)^2}{12} - \frac{(K-H)(2H-K)}{6},$$

in which the left side is certainly not less than Δ^2 , as appears from the first inequality of (1), which gives $(K-H)/6$ to be at least as great as $\Delta/\sqrt{3}$. The proof of the second inequality in (2) is merely an exercise in finding the minimum of a function of 2 independent variables. It should be noted that the second inequality in (1) or (2) is of no value in case $5H \geq 3K$, since then the lower estimate which it gives for $\Delta\sqrt{3}$ or Δ^2 is not even positive. It will be shown at the end when this case actually arises. It is, of course, to be understood in both (1) and (2) that the sign of equality never applies except when the triangle is equilateral, when it must be used throughout.

2. Analytical statement of the problem. Since all the quantities in (2) are homogeneous and of degree 4 in the sides, we may take any one of them, say c , to be unity, and since the other 2 sides, a and b , are subject to the inequalities

$$a + b > 1 > a - b > -1,$$

we know that the point with coordinates (a, b) must lie to the right of the line $x + y = 1$ and within the strip bounded above by the line $y = x + 1$ and below by the line $y = x - 1$. That is, we may take

$$(3) \quad a = u + v, \quad b = 1 - u + v,$$

where u is a proper fraction and v is positive.

It follows that

$$(4) \quad \frac{(K - H)}{2} = v + u - u^2$$

is positive, while

$$(5) \quad (2H - K) = (v - \frac{1}{2})^2 + 3(u - \frac{1}{2})^2$$

is also positive, except that it is zero when $u = v = \frac{1}{2}$, which corresponds to the case in which the triangle is equilateral. Of course, also

$$(6) \quad \Delta^2 = (u - u^2)(v + v^2).$$

Since Δ^2 and $(K - H)^2/12$ have the same value, namely $3/16$, when the triangle is equilateral, it is natural to try out $(K - H)^2/12$ as an upper estimate for Δ^2 and to attempt to construct a lower estimate of the form

$$\frac{(K - H)^2}{12} - \lambda(K - H)(2H - K),$$

with λ positive and taken sufficiently large, seeing that $(2H - K)$ is known to be zero when the triangle is equilateral. For $u = \frac{1}{2}$ and v only slightly positive, which implies that Δ^2 is also only slightly positive, we see that λ must be chosen so as to make

$$\lambda(2H - K) - \frac{(K - H)}{12} > 0.$$

But since $(K - H)$ barely exceeds $\frac{1}{2}$ while $(2H - K)$ is only slightly less than $\frac{1}{4}$, this implies that λ must be taken not less than $\frac{1}{6}$. This is the reason for expecting

$$\frac{(K - H)^2}{12} - \frac{(K - H)(2H - K)}{6}$$

to turn out to be a lower estimate for Δ^2 , as stated in (2).

This reduces the problem to a study of the function

$$(7) \quad T = \Delta^2 - \frac{(K - H)^2}{12} + \frac{(K - H)(2H - K)}{6}$$

in the region of the (u, v) -plane bounded left and right by $u = 0$ and $u = 1$ respectively and below by $v = 0$. At points $(0, v)$ or $(1, v)$ on the left or right boundaries of this (u, v) -region

$$(8) \quad T = \frac{v(v - 1)^2}{3},$$

while at points $(u, 0)$ on the lower boundary

$$(9) \quad T = \frac{(u - u^3)(2u - 1)^2}{3}.$$

In other words, the function T is positive all along the boundary of the (u, v) -region except at the points $(0, 1)$, $(0, 0)$, $(\frac{1}{2}, 0)$, $(1, 0)$, $(1, 1)$, where it is in every case zero. For points (u, v) taken within the (u, v) -region it remains to show that zero is the least value of T and that it arises nowhere else than at $(\frac{1}{2}, \frac{1}{2})$, where it is easy to verify from (4), (5), (6) that it does arise.

3. Minimum value of T in the (u, v) -region. Employing a dash to denote derivation and a subscript to indicate the variable with respect to which it is done, we readily find that

$$(10) \quad T'_u = \frac{4}{3}(1 - 2u)[(v - \frac{3}{8})^2 + 2(u - \frac{1}{2})^2 - \frac{25}{64}],$$

$$(11) \quad T'_v = (v - \frac{1}{3})(v - 1) + \frac{8}{3}(v - \frac{3}{8})(u - u^2).$$

On putting $T'_u = 0$, $T'_v = 0$, we obtain the following 6 points in the (u, v) -domain:

(i) $u = \frac{1}{2}, v = \frac{1}{2};$

(ii) $u = \frac{1}{2}, v = \frac{1}{6};$

(iii) 4 points arising from

$$(v - \frac{3}{8})^2 + 2(u - \frac{1}{2})^2 = \frac{25}{64}, \quad (v - \frac{1}{3})(v - 1) + \frac{8}{3}(v - \frac{3}{8})(u - u^2) = 0,$$

in which u is different from $\frac{1}{2}$.

For point (i)

$$T''_{uu} = 1, \quad T''_{uv} = 0, \quad T''_{vv} = \frac{1}{3},$$

indicating that T has a minimum value there, namely zero.

For point (ii)

$$T''_{uu} = \frac{25}{27}, \quad T''_{uv} = 0, \quad T''_{vv} = -\frac{1}{3},$$

indicating that T has neither a maximum or minimum there, the actual value being positive, however, namely $1/162$. The first equation under (iii) represents the ellipse

$$(12) \quad (v - \frac{3}{8})^2 + 2(u - \frac{1}{2})^2 = \frac{25}{64},$$

with centre at the point $u = \frac{1}{2}, v = \frac{1}{2}$. The portion of this ellipse extending from $v = 0$ to $v = 1$ is all that we need consider, since v is negative on the remaining portion. The result of eliminating u between (12) and the second equation of (iii), namely,

$$(13) \quad (v - \frac{1}{3})(v - 1) + \frac{8}{3}(v - \frac{3}{8})(u - u^2) = 0,$$

is the cubic equation

$$(14) \quad 32v^3 - 12v^2 - 15v + 5 = 0,$$

which obviously has one negative root and is shown by Sturm's Theorem to have two positive roots, one between 0 and $\frac{1}{2}$ and the other between

$\frac{3}{4}$ and 1. Each of these two positive values of v gives 2 points under (iii), both lying on the ellipse (12) and each the image of the other in its major axis $u = \frac{1}{2}$. This accounts for the 4 points under (iii).

For all these 4 points (u, v)

$$T''_{uu} = -\frac{8}{3}(1-2u)^2, \quad T''_{uv} = (1-2u)(\frac{8}{3}v-1), \quad T''_{vv} = -1+v+\frac{4}{3}v^2,$$

from which it follows that

$$T''_{uu}T''_{vv} - T''_{uv}T''_{vu} = \frac{(1-2u)^2(5+8v-32v^2)}{3},$$

when use is made of equation (12) to reduce the second factor to make it involve v only. It appears that the sign of $T''_{uu}T''_{vv} - T''_{uv}T''_{vu}$ at any of the 4 points (u, v) is opposite to that of the slope of the cubic curve

$$(15) \quad Z = 32v^3 - 12v^2 - 15v + 5$$

at the corresponding points where it crosses the axis $Z = 0$. For the greater of these two values of v the slope of the curve is positive, which means that $T''_{uu}T''_{vv} - T''_{uv}T''_{vu}$ is negative, thus indicating that T has neither a maximum or minimum at either of the 2 points of (iii) associated with this greater value of v . For the lesser of these two values of v , however, the slope of the curve is negative, which in turn implies that $T''_{uu}T''_{vv} - T''_{uv}T''_{vu}$ is positive, thus indicating that T has a maximum at both of these 2 points of (iii) associated with this lesser value of v , since, indeed, the common sign of T''_{uu} and T''_{vv} is negative. Hence, the only point in the (u, v) -region making T a minimum is the point (i), which gives it the value zero. It follows that every point in the (u, v) -region makes T positive. This completes the proof of the second inequality of (2).

4. Final remarks. The second inequalities of (1) and (2) are both based on the use of the elementary symmetric functions $2s$ and K , to the exclusion of the use of the third elementary symmetric function abc . It is natural for the discussion in (2) to adopt the limitation in this regard that is characteristic of the discussion in (1), since if abc were admitted as well as $2s$ and K there would be no need for inequalities at all in (2), seeing that Δ^2 is rationally expressible in terms of $2s$, K , and abc .

The first inequality in (2) is more satisfactory than the second, for the reason that the first involves v to the square power on both sides while the second involves v to the square power on one side and to the cube power on the other. This may be contrasted with the inequalities in (1), where the powers of v are linear on both sides in the first inequality but linear and square on opposite sides in the second inequality.

It remains to indicate when $5H \geq 3K$, which is the condition for the lower estimate in (1) or (2) to be zero or negative and so to be of no value whatever. The inequality is equivalent to

$$(2H - K) \geq \frac{(K - H)}{2},$$

which by (4) and (5) reduces to

$$(16) \quad (v-1)^2 + 4(u-\tfrac{1}{2})^2 \geq 1.$$

This means that the lower estimate is zero or negative and so of no account for points in the (u, v) -region on or without the ellipse

$$(17) \quad (v-1)^2 + 4(u-\tfrac{1}{2})^2 = 1,$$

which lies wholly within the (u, v) -region except for the points $(0, 1)$, $(\tfrac{1}{2}, 0)$, $(1, 1)$ which belong to its left, bottom, and right boundaries respectively. In other words, the points for which the second inequality is of any value at all fill only an infinitesimal part of the whole (u, v) -region.

REFERENCES

1. J. C. H. Gerretsen, *Nieuw Tijdschr. Wiskunde*, 41 (1953), 1-7.
2. R. Weitzenböck, *Math. Z.*, 5 (1919), 137-146.
3. P. Finsler and H. Hadwiger, *Comment. Math. Helv.*, 10 (1938), 316-326.



Tangents to Ovals with Two Equichordal Points*

By LLOYD DULMAGE

Presented by R. L. JEFFERY, F.R.S.C.

A point is called an equichordal point, or simply an e -point of a closed curve if every line through the point meets the curve in two points a constant distance apart. It has been conjectured that no closed curve has two distinct e -points. Such curves have been discussed by W. Süss (2) and G. A. Dirac (1). Dirac showed that no such convex curve exists for which the ratio a of the distance between the e -points to the constant chord length is $\geq \sqrt{3}/2$, and stated that he had made computations which established that no such curve exists for $a > 0.4$. He showed further that every such convex curve has a continuously varying tangent.

In this note, we call a closed oval with continuously varying tangent and two e -points an e -curve. We establish some tangent properties for e -curves and hence show that no such curve exists for $a \geq 2\sqrt{2}/3\sqrt{3}$.

Dirac has shown, without using convexity, that, if the e -points are R and S , the curve meets RS in A and B such that RS and AB have the same mid-point, and the curve lies between perpendiculars to RS at A and B . For an e -curve, then, the tangents at A and B are perpendicular to RS . For convenience we take the length of the chords to be unity so that $RS = a$.

Consider chords through S meeting an e -curve in P and Q . Let $SP = r$, $SQ = s$, and let the tangents to the e -curve make acute angles α and β with PQ at P and Q respectively. These acute angles fall on the same side of PQ . Let angle $PSA = \theta$. Since $r + s = 1$, we have

$$\frac{dr}{d\theta} + \frac{ds}{d\theta} = 0,$$

r and s being differentiable functions of θ , since an e -curve has a continuously varying tangent. We have

$$\tan \alpha = \frac{r}{\pm \frac{dr}{d\theta}},$$

the plus sign applying when r is an increasing function of θ and the minus sign when r is a decreasing function of θ . Similarly

$$\tan \beta = \frac{s}{\pm \frac{ds}{d\theta}},$$

*The research resulting in this note was carried out at the Summer Research Institute of the Canadian Mathematical Congress, 1953.

and consequently, since one of r and s increases when the other decreases,

$$(1) \quad \frac{\tan \alpha}{\tan \beta} = \frac{r}{s}.$$

Consider the chords P_1SP_2 , P_2RP_3 , P_3SP_4 , ... giving rise to a sequence of points $\{P_n\}$, each with a tangent (Figure 1). The acute angles α_1 and β_1 are related as in (1). Consider the 3 cases,

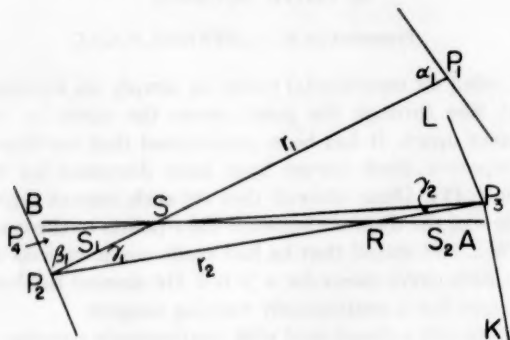


FIGURE 1

(a) If $\beta_1 + \gamma_1 < 90^\circ$, then $\beta_1 + \gamma_1 = \alpha_2$ (the acute angle between the tangent at P_2 and P_2P_3). Hence β_2 is the acute angle RP_3L .

(b) If $\beta_1 + \gamma_1 > 90^\circ$, then $180^\circ - (\beta_1 + \gamma_1) = \alpha_2$ and β_2 is the acute angle RP_3K .

(c) If $\beta_1 + \gamma_1 = 90^\circ$, then the tangent at P_3 is perpendicular to P_2P_3 . If case (a) occurs then α_3 is $LP_3S = \beta_2 - \gamma_2$ and if $r_n > s_n$ for $n > 2$, it follows directly using (1) and considering successive tangents that $\beta_n \rightarrow 0$. In case (c) if $r_n > s_n$ for $n > 2$, $\beta_n + \gamma_n$ is acute and $\beta_n \rightarrow 0$. This implies a discontinuity in the variation of the tangent at A . Accordingly we have the lemma,

(2) If, in the sequence of tangents associated with the points P , there exists N such that $\beta_N + \gamma_N < 90^\circ$ and $r_n > s_n$ for $n > N$, then no e -curve exists through the points P_n with these tangents.

We now establish the lemma,

(3) All e -curves through the point P with the same e -points R and S have the same tangent at P .

If P is A or B the tangent is perpendicular to RS . If P is not A or B , suppose we have two distinct tangents at P and consider the sequence of points $\{P_n\}$ arising from $P = P_1$. Let $\{\beta_n'\}$ and $\{\beta_n''\}$ be the sequences of angles arising from the two tangents. Since there exists N such that $r_n > s_n$ for $n > N$, it follows from (2) that $\beta_n' + \gamma_n > 90^\circ$ and $\beta_n'' + \gamma_n > 90^\circ$ for $n > N$. We have $\beta_n', \beta_n'' < 90^\circ$, and hence $|\beta_n'' - \beta_n'| < \gamma_n$ for $n > N$.

N may be chosen so that $\beta_n', \beta_n'', \alpha_n', \alpha_n''$ are all $> 45^\circ$. Suppose, for definiteness $\beta_{n-1}' > \beta_{n-1}''$ so that $\alpha_n'' > \alpha_n'$ and $\beta_n'' > \beta_n'$. We have

$$(\tan \beta_n'' - \tan \beta_n')(1 - \tan \beta_n' \tan \alpha_n'') < 0.$$

Using

$$\frac{\tan \alpha_n'}{\tan \beta_n'} = \frac{\tan \alpha_n''}{\tan \beta_n''} = \frac{r_n}{s_n} > 1,$$

we have

$$\tan \beta_n'' + \tan \beta_n' \tan \beta_n'' \tan \alpha_n' < \tan \beta_n' + \tan \beta_n'' \tan \beta_n' \tan \alpha_n''$$

$$\frac{\frac{r_n}{s_n} - 1}{\frac{1}{\tan \beta''} + \tan \alpha''} < \frac{\frac{r_n}{s_n} - 1}{\frac{1}{\tan \beta'} + \tan \alpha'}$$

$$\tan(\alpha_n'' - \beta_n'') < \tan(\alpha_n' - \beta_n').$$

Accordingly $\alpha_n'' - \alpha_n' < \beta_n'' - \beta_n'$ for $n > N$. Clearly

$$\alpha_n'' - \alpha_n' = \beta_{n-1}' - \beta_{n-1}'', \quad n > N + 1,$$

so that

$$|\beta_{n-1}'' - \beta_{n-1}'| < |\beta_n'' - \beta_n'|, \quad n > N + 1.$$

Since

$$\beta_n'' - \beta_n' < \gamma_n \text{ and } \gamma_n \rightarrow 0,$$

we have a contradiction. Lemma (3) is established.

Now let O be the mid-point of RS and consider the point P_1 of intersection

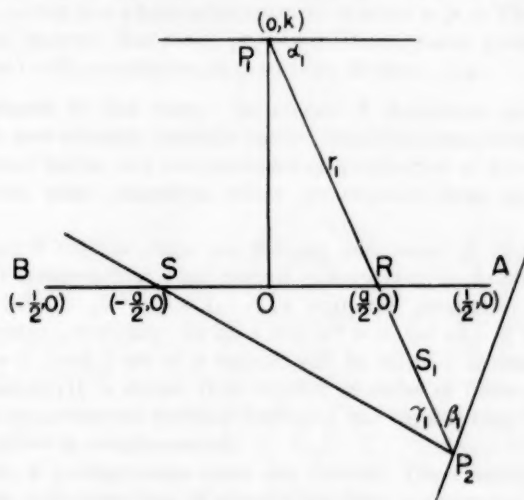


FIGURE 2

of an e -curve and the perpendicular to RS at O . The tangent at P_1 is parallel to RS for if not, a reflection in P_1O would yield two distinct tangents to e -curves through P_1 , contrary to (3). Assign coordinates as in Figure 2. The condition $\beta_1 + \gamma_1 \leq 90^\circ$ or $\tan(\beta_1 + \gamma_1) > 0$ is satisfied provided $r_1^3 - r_1^2 + a^2/2 \geq 0$. Since r_1 is between 0 and 1, $r_1^3 - r_1^2$ is $> -4/27$ and the condition is satisfied provided $a \geq 2\sqrt{2/3}\sqrt{3}$. Since, for these values of a , $r_n > s_n$ for $n > 1$, we see from (2) that no e -curve exists.

REFERENCES

1. G. A. Dirac, *Ovals with equichordal points*, J. London Math. Soc., 27 (1952), 429-437.
2. W. Süss, *Eibereiche mit ausgezeichneten Punkten*, Tohoku Math. J., 25 (1925), 86-98.

Coordinates in Geometry

K. D. FRYER and ISRAEL HALPERIN, F.R.S.C.

1. INTRODUCTION

1.1. In all of what follows n will denote a fixed positive integer and left modules will always mean left modules of the set V of all vectors $u = (\alpha^1, \dots, \alpha^n)$ of length n . The coordinates α^i will be arbitrary elements in a ring \mathfrak{R} .

If \mathfrak{R} is a division ring it is well known that the set of all left modules of V form a complemented modular lattice. If \mathfrak{R} , more generally, is a regular ring with unit element, then a complemented modular lattice is formed by all left modules of *finite span* (a left module is of finite span if it is spanned by a finite number of vectors). In the case that \mathfrak{R} is a division ring every left module is of finite span.

The main theorem of this note is concerned with the converse to the previous statements due to J. von Neumann (2, Theorem 14.1), i.e. an arbitrary given complemented modular lattice can be represented (coordinatized) as such a lattice of all left modules of finite span (using vectors of length n with coordinates in a suitable regular ring with unit element) if the given lattice has a homogeneous basis of order $n \geq 4$. This generalizes the classical theorem that every projective Desarguesian geometry can be coordinatized with coordinates in a suitable division ring.

1.2. Contents of this note. In section 2 definitions are given for: lattice with zero element, modular lattice, relatively complemented lattice, complemented lattice and independence of a collection of lattice elements, together with some properties which are required later and are easily verified.

In section 3 regular rings are defined and some of their properties obtained. It is shown that a left module of finite span is always spanned by n vectors $(\alpha^{j1}, \dots, \alpha^{jn})$, $j = 1, \dots, n$ with the properties: for each j , α^{jj} is idempotent, $= e^j$, say; for all $i > j$, $\alpha^{ji} = 0$; for all $i < j$, $e^j \alpha^{ji} = \alpha^{ji}$ and $\alpha^{ji} e^i = 0$. Such a set of n vectors will be called a *canonical basis* for the left module. It is shown that the left modules of finite span form a relatively complemented modular lattice; if the regular ring \mathfrak{R} has a unit then this lattice is complemented.

In section 4 homogeneous bases are defined. The classical method of constructing a division ring of coordinates from a projective geometry is generalized, in a lattice theoretic form, so as to obtain a ring of coordinates \mathfrak{R} (which is regular and has a unit) from a given complemented modular

lattice L if the lattice possesses a homogeneous basis of order $n \geq 4$. The ring \mathfrak{R} is called an auxiliary ring of L .

In another paper, to be published under the title "On the coordinatization theorem of J. von Neumann" we assume that L has a homogeneous basis of order $n \geq 4$ and an auxiliary ring \mathfrak{R} and we give a rule which assigns to each x in L a family of left modules. We then prove that all left modules, assigned by this rule to the same x , actually coincide and that the rule sets up a (1, 1) order preserving correspondence (i.e. a lattice isomorphism) between L and the set of all left modules of finite span. This establishes the von Neumann coordinatization theorem stated in 1.1.

This note should be considered as an exposition of parts of (1, 2). However we introduce some simplifications and find it desirable to give a complete exposition.

1.3. Notation. Greek letters $\alpha, \beta, \gamma, \dots$, (but excluding π) without subscripts will denote elements in a ring \mathfrak{R} ; e, f, g will be reserved for ring elements which are idempotent. For fixed $\alpha^1, \alpha^2, \dots, (\alpha^1, \alpha^2, \dots)_l$ will denote the left ideal consisting of all finite sums $\beta^1 \alpha^1 + \beta^2 \alpha^2 + \dots$ with arbitrary β^i in \mathfrak{R} ; similarly $(\alpha^1, \alpha^2, \dots)_r$ will denote the right ideal of elements $\alpha^1 \beta^1 + \alpha^2 \beta^2 + \dots$. The letters u, v, \dots will denote vectors of length n with coordinates in \mathfrak{R} and $(u, v, \dots)_l$ will denote the left module spanned by u, v, \dots which consists of all finite sums $\alpha u + \beta v + \dots$ with arbitrary α, β, \dots in \mathfrak{R} . The letters $a, b, c, d, \dots, x, y, z, \dots, p, q, w, \dots, A, B, S, R, \dots$ will denote elements in a lattice L . The letters i, j, k, m, s, t, \dots will denote positive integers. The same symbols 0, 1 will be used to denote ring elements and lattice elements but there will be no ambiguity. The symbols $+$, \sum will denote addition for ring elements and lattice join (i.e. supremum) for lattice elements but there will be no ambiguity. Similarly $\alpha\beta$ and $\pi\alpha^j$ will denote ring multiplication whereas xy and $\pi_j x^j$ will denote lattice meet (i.e. infimum). With each ring element α there will be associated certain lattice elements to be denoted by α with subscripts, thus α_{ij}, α_i^0 , and α_j' .

2. COMPLEMENTED MODULAR LATTICES

2.1. Lattices. A lattice with zero L is a collection of elements 0, $a, b, c, \dots, x, y, z, \dots$ partially ordered by a relation $a \leq b$ (also written $b \geq a$) such that $0 \leq x$ for every x and for each pair a, b there are elements $a+b$ and ab (necessarily unique) satisfying:

$$\begin{aligned} a+b &\leq x && \text{if and only if } a \leq x \text{ and } b \leq x, \\ x &\leq ab && \text{if and only if } x \leq a \text{ and } x \leq b. \end{aligned}$$

$L(a)$ will denote the sub-lattice with zero of all $x \leq a$.

2.2. Modular lattices. L is called a modular lattice if: $a(b+c) = b+ac$ for all a, b, c with $b \leq a$. This modular law implies the absorption law: $ab+c = a(b+c)$ for all a, b, c , with $c(a+b) = 0$; the clipping identity: $a(b+c) = a\{b(a+c) + c\}$ for all a, b, c ; and the superfluous term identity: $ab = a(b+c) = abd$ for all a, b, c, d with $c(a+b) = 0$ and $b \leq d$. Appli-

cations of these identities will be indicated by (ML), (AL), (CI) and (ST) respectively.

2.3. Independence. In a modular lattice with zero, for each $m = 1, 2, \dots$, elements x^1, \dots, x^m are called independent if for each $i \leq m$, $x^i(x^1 + \dots + x^{i-1} + x^{i+1} + \dots + x^m) = 0$. If for some ordering of the x^i it is true that $x^j(x^1 + \dots + x^{j-1}) = 0$ for all $j \leq m$ then the x^i are necessarily independent. If the x^i are independent and for each of a finite number of j , I_j is a subset of the integers $1, 2, \dots, m$, then

$$\pi_j(\sum x^i; i \text{ in } I_j) = (\sum x^i; i \text{ in all } I_j);$$

this is a special case of the more general theorem that if the x^i are independent and $x^{ij} \leq x^i$ for each of a finite number of j , then

$$\pi_j \sum_i x^{ij} = \sum_i \pi_j x^{ij}.$$

The symbols $\oplus, \sum \oplus$ will sometimes be used in place of $+, \sum$ to imply independence of the elements involved.

A detailed treatment of this (von Neumann) independence is given in (1).

2.4. Relative complements and complements. If $x \leq z$ in a lattice L with zero then a relative complement, or inverse, of x in z is an element y (not necessarily unique) such that $x \oplus y = z$; $[z - x]$ will be used to denote an inverse of x in z . A lattice L with zero is called relatively complemented if there exists at least one relative complement of x in z whenever $x \leq z$.

A lattice L is said to have a unit 1 (necessarily unique) if $x \leq 1$ for all x in L . If L has zero and unit elements then a relative complement of x in 1 is also called a complement of x ; L is called complemented if each x has at least one complement.

A relatively complemented lattice with unit is obviously complemented; on the other hand, a complemented *modular* lattice is also relatively complemented (indeed, if $x \leq z$ and y is a complement of x then yz is a relative complement of x in z).

The *indivisibility of inverses* follows from the modular law: i.e., if y_1 and y_2 are both inverses of a in b and $y_1 \leq y_2$ then $y_1 = y_2$. Because of this fact, to be indicated by: (I of I), it is possible to replace "points" as used in certain constructions in the classical theory of projective geometry, by "inverses".

2.5. Perspectivities. Elements x^1 and x^2 in a lattice with zero are called perspective if they possess a common inverse in $x^1 + x^2$. Any such common inverse b is called an axis of perspectivity and, if the lattice is modular, sets up a (1, 1) order preserving mapping (called a perspective mapping) of $L(x^1)$ onto $L(x^2)$:

$$\text{if } z^1 \leq x^1, \text{ then } z^1 \rightarrow (z^1 + b)x^2,$$

$$\text{if } z^2 \leq x^2, \text{ then } z^2 \rightarrow (z^2 + b)x^1.$$

If z^1 and z^2 correspond under this mapping then $z^1 + b = z^2 + b$.

3. REGULAR RINGS

(This section is based on (2, chap. II))

3.1. Definition of regular ring. A regular ring \mathfrak{R} is a ring *not necessarily with unit* such that for each α in \mathfrak{R} , $\alpha\beta\alpha = \alpha$ for at least one β in \mathfrak{R} . It is easy to prove that a ring is a regular ring if and only if for each α , the principal left ideal $(\alpha)_l$ can be represented as $(e)_l$ for some idempotent e and if and only if for each α , the principal right ideal $(\alpha)_r$ can be represented as $(f)_r$ for some idempotent f (if $\alpha\beta\alpha = \alpha$ then $(\alpha)_l = (\beta\alpha)_l$, $(\alpha)_r = (\alpha\beta)_r$ and $\beta\alpha$, $\alpha\beta$ are idempotents). If \mathfrak{R} is regular then α is contained in $(\alpha)_l$ and in $(\alpha)_r$.

3.2. Principal left ideals. (Throughout this paper, right and left may obviously be interchanged). In a regular ring the principal left ideals form a relatively complemented modular lattice with zero (complemented, if \mathfrak{R} has a unit) when partially ordered by inclusion; the zero (left principal ideal) of this lattice consists of the zero element of \mathfrak{R} only. This is easily verified since, if e, f are idempotents,

(i) the smallest left ideal containing $(e)_l$ and $(f)_l$ is precisely $(e + g)_l$ where g is any idempotent with $(g)_l = (f - fe)_l$,

(ii) the left ideal of all ring elements common to $(e)_l$ and $(f)_l$ is precisely $(f - gf)_l$ where g is any idempotent with $(g)_r = (f - fe)_r$,

(iii) $(f - fe)_l$ is a relative complement of $(e)_l$ in $(f)_l$ whenever $(e)_l$ is contained in $(f)_l$,

(iv) if \mathfrak{R} has a unit 1 then $(1)_l \geq (e)_l$.

It is now easy to prove that: a ring \mathfrak{R} is regular if and only if its principal left ideals form a relatively complemented modular lattice such that every principal left ideal $(a)_l$ is contained in a principal left ideal $(e)_l$ with e idempotent (possibly depending on a); and a ring \mathfrak{R} with unit is regular if and only if its principal left ideals form a complemented modular lattice.

3.3. Ring conditions on α . If g is an idempotent in a regular ring \mathfrak{R} and $\beta^i, \gamma^i, i = 1, \dots, m$ are in \mathfrak{R} , then the conditions on α : α is in $(g)_l$ and $\alpha\beta^i$ is in $(\gamma^i)_l$ for each i , are equivalent to: α is in $(e)_l$ for a suitable idempotent $e = e(g, \beta^1, \dots, \gamma^1, \dots)$.

By 3.2 (ii) it is sufficient to prove this for the case $m = 1$. We write β for β^1 and γ for γ^1 and we may clearly suppose that γ is idempotent. Then the conditions on α are equivalent to: $\alpha = \alpha g$ and $\alpha(\beta - \beta\gamma) = 0$, that is, to the conditions: $\alpha = \alpha g$, $\alpha f = 0$ where f is an idempotent with $(f)_r = (\beta - \beta\gamma)_r$, that is, to the condition: α is in $(g - hg)_l$ where h is any idempotent with $(h)_r = (gf)_r$.

3.4. Canonical basis. If M is a left module of finite span (of vectors of length n with coordinates in a ring \mathfrak{R}) then M is certainly spanned by a finite number of vectors $v^j = (\alpha^j_1, \dots, \alpha^j_n)$. If \mathfrak{R} is regular, then M is always spanned by a canonical basis (see 1.2), as we shall now verify.

Starting from the given v^j which span M , there is an idempotent e^n with $(e^n)_l = (\alpha^{1n}, \alpha^{2n}, \dots)_l$ (this implies $\alpha^{jn} e^n = \alpha^{jn}$ for all j and $\sum_j \beta^j \alpha^{jn} = e^n$

for suitable β^j). By replacing v^1 by $\sum_k \beta^k v^k$ and v^j (for $j > 1$) by $v^j - \alpha^{jn}(\sum_k \beta^k v^k)$ we obtain a new finite set of vectors (which we denote again as v^j) which span M and have the additional properties: $\alpha^{1n} = e^n$ (idempotent) and $\alpha^{jn} = 0$ for all $j > 1$. Now replace v^1 by the two vectors $e^n v^1$ and $v^1 - e^n v^1$ (this increases the number of vectors used to span M but the number remains finite). Then we may suppose that the v^j have the additional property: $e^n \alpha^{1i} = \alpha^{1i}$ for all i .

Now apply the procedure of the preceding paragraph to the vectors v^j ($j \geq 2$) to obtain an idempotent e^{n-1} so that the vectors which span M may be supposed to have the additional properties: $\alpha^{2,n-1} = e^{n-1}$, $\alpha^{j,n-1} = 0$ for $j > 2$ and $e^{n-1} \alpha^{2,i} = \alpha^{2,i}$ for all i . Successive repetitions of this procedure show that M can be spanned by vectors v^j (necessarily n in number) with $\alpha^{jj} = e^j$ (idempotent), $\alpha^{ji} = 0$ for all $i > n + 1 - j$ and $e^j \alpha^{ji} = \alpha^{ji}$ for all i, j .

Then v^1 may be replaced by $v^1 - \alpha^{1,n-1} v^{n-1}$ giving the additional property $\alpha^{1,n-1} e^{n-1} = 0$. By repetition of this procedure we may assume that $\alpha^{1,i} e^i = 0$ for all $i < n$. Similarly we may assume that $\alpha^{ji} e^i = 0$ for all $i < n + 1 - j$.

Then, if u^j is defined to be v^{n+1-j} , the u^j are a canonical basis for M .

3.5. Vector conditions on α . Suppose g is an idempotent in a regular ring \mathfrak{R} and for each $i = 1, \dots, m$ suppose M^i is a left module of finite span and v^i is a given vector. Then the conditions on $\alpha : \alpha$ is in $(g)_l$ and αv^i is in M^i for each i , are equivalent to: α is in $(e)_l$ for a suitable idempotent $e = e(g, v^1, \dots, M^1, \dots)$.

By 3.2 (ii) it is sufficient to prove this for the case $m = 1$. We write $v^1 = v = (\alpha^1, \dots, \alpha^n)$ and we may suppose that M^1 has a canonical basis $u^j = (\alpha^{j1}, \dots, \alpha^{jn})$, $j = 1, \dots, n$. Then the conditions on α are equivalent to: (i) α is in $(g)_l$ and (ii) $\alpha v = \sum_k \beta^k u^k$ for suitable β^k . But if such β^k exist then $\alpha \alpha^j \alpha^{jj} = \beta^j \alpha^{jj}$ for all j . Hence condition (ii) on α may be written: $\alpha v = \sum_j \rho^j \alpha^j u^j$ and is equivalent to the n conditions: $\alpha(\alpha^k - \sum_j \alpha^j \alpha^{jk}) = 0$, $k = 1, \dots, n$. It is now sufficient to apply the result of 3.3.

3.6. The lattice of left modules of finite span. If \mathfrak{R} is a regular ring the left modules of finite span form a relatively complemented modular lattice L when partially ordered by inclusion; if the regular ring \mathfrak{R} has a unit then L has a unit and hence is complemented (note that the vector $u = (\alpha^1, \dots, \alpha^n)$ is always in $(u)_l$ if \mathfrak{R} is regular for $eu = u$ with e any idempotent such that $(e)_r = (\alpha^1, \dots, \alpha^n)_r$). This is now easily verified, using the following statements:

- (i) L has a zero (left module of finite span) consisting of the zero vector $(0, \dots, 0)$ only.
- (ii) If M^1 is a left module spanned by u^{11}, \dots, u^{1n} and M^2 is a left module spanned by u^{21}, \dots, u^{2n} , then the smallest left module containing M^1 and M^2 is spanned by $u^{11}, \dots, u^{1n}, u^{21}, \dots, u^{2n}$.
- (iii) If M^1 and M^2 are left modules with canonical bases $u^{1j} = (\alpha^{1j1}, \dots, \alpha^{1jn})$, $j = 1, \dots, n$ and $u^{2j} = (\alpha^{2j1}, \dots, \alpha^{2jn})$, $j = 1, \dots, n$ respect-

ively, then the vectors common to M^1 and M^2 (clearly a left module) actually form a left module of finite span. To prove this by induction on n (for $n = 1$ this is implied by (ii) of 3.2) it is sufficient to show that the coordinates α^n in all vectors $(\alpha^1, \dots, \alpha^n)$ common to M^1 and M^2 form a principal left ideal.

For any such α^n it is clear that $\alpha^n \alpha^{1nn} = \alpha^n \alpha^{2nn} = \alpha^n$ so that, without changing the set of vectors common to M^1 and M^2 , the vectors u^{1n} and u^{2n} may be replaced by $e^n u^{1n}$ and $e^n u^{2n}$ respectively where e^n is any idempotent with $(e^n)_i = (\alpha^{1nn})_i (\alpha^{2nn})_i$. Thus we may suppose that $\alpha^{1nn} = \alpha^{2nn} = e^n$. (For ease in writing we shall use h to mean $n - 1$.) Then the necessary and sufficient conditions that α be the n th coordinate in a vector common to M^1 and M^2 are: (i) α is in $(e^n)_i$ and (ii) for some $\alpha^1, \dots, \alpha^h, \beta^1, \dots, \beta^h, \gamma^1, \dots, \gamma^h$,

$$\begin{aligned} (\alpha^1, \dots, \alpha^h) &= \sum_{j=1}^h \beta^j (\alpha^{1j1}, \dots, \alpha^{1jh}) + \alpha (\alpha^{1n1}, \dots, \alpha^{1nh}) \\ &= \sum_{j=1}^h \gamma^j (\alpha^{2j1}, \dots, \alpha^{2jh}) + \alpha (\alpha^{2n1}, \dots, \alpha^{2nh}). \end{aligned}$$

The condition (ii), which involves vectors of length $h = n - 1$, is equivalent to (the $\alpha^1, \dots, \alpha^h$ may be ignored): αv is in M where v is the vector $(\alpha^{1n1} - \alpha^{2n1}, \dots, \alpha^{1nh} - \alpha^{2nh})$ and M is the left module spanned by $2n - 2$ vectors of length $n - 1$, $(\alpha^{1j1}, \dots, \alpha^{1jh}), (\alpha^{2j1}, \dots, \alpha^{2jh}), j = 1, \dots, n - 1$. It is now sufficient to apply the result of 3.5.

(iv) Suppose M^1 and M^2 are left modules with canonical bases $u^{1j} = (\alpha^{1j1}, \dots, \alpha^{1jn}), j = 1, \dots, n$ and $u^{2j} = (\alpha^{2j1}, \dots, \alpha^{2jn}), j = 1, \dots, n$ respectively and suppose M^1 is contained in M^2 .

Then for each j , $(\alpha^{1jj})_i$ is contained in $(\alpha^{2jj})_i$. A relative complement of M^1 in M^2 may be obtained as M , the left module spanned by u^1, \dots, u^n with $u^j = (\alpha^{2jj} - \alpha^{1jj} \alpha^{1jj}) u^{2j}$. For clearly this M is a left module of finite span and is contained in M^2 . Next, M and M^1 have only the zero vector in common; for if

$$w = \sum_{j=1}^n \beta^j u^j = \sum_{j=1}^n \gamma^j u^{1j}$$

then, equating the n th coordinates, we obtain $\beta^n (\alpha^{2nn} - \alpha^{1nn} \alpha^{1nn}) = \gamma^n \alpha^{1nn}$; multiplying on the right with the idempotent α^{1nn} shows that both sides of this equality are zero and hence:

$$w = \sum_{j=1}^{n-1} \beta^j u^j = \sum_{j=1}^{n-1} \gamma^j u^{1j}.$$

Successive reductions show that $w = 0$, as stated. Finally M^2 is contained in $M \oplus M^1$ (and hence $M^2 = M \oplus M^1$): for the identity:

$$u^{2j} = u^j + \alpha^{2jj} u^{1j} + (\alpha^{2jj} \alpha^{1jj} u^{2j} - \alpha^{2jj} u^{1j})$$

shows that u^{2j} = vector in M + vector in M^1 + v where v is a vector in M^2 with i th coordinate zero for all $i > j$. Thus by induction on k , every vector in M^2 with at most the first k coordinates different from zero, is contained in $M + M^1$; when k takes the value n , we obtain: M^2 is contained in $M \oplus M^1$, as stated.

(v) If R has a unit 1, then L clearly has as unit (left module of finite span) the left module spanned by u^1, \dots, u^n with $u^j = (\alpha^{j1}, \dots, \alpha^{jn})$, $\alpha^{ji} = 0$ if $j \neq i$, $= 1$ if $j = i$.

4. THE AUXILIARY RING

(This section is based on (2, chap. IV-IX))

4.1. Homogeneous basis and normalized frame. Let L be a complemented modular lattice. Then a_1, \dots, a_n will be called a *homogeneous basis of order n* for L if $a_1 \oplus \dots \oplus a_n = 1$ and a_i is perspective to a_j for all i, j . Suppose that for such a homogeneous basis, a_1 is perspective to a_i with axis x_i for $i = 1, \dots, n$ (clearly $x_1 = 0$): set

$$c_{ij} = c_{ji} = (x_i + x_j)(a_i + a_j)$$

for all i, j . Then the c_{ij} , $i, j = 1, \dots, n$ have the properties: for all i, j, k ,

$$(4.1.1) \quad c_{ij} = c_{ji}; \quad c_{ii} = 0; \quad (c_{ij} + c_{jk})(a_i + a_k) = c_{ik}; \\ a_i \oplus c_{ij} = a_j \oplus c_{ij}.$$

A homogeneous basis a_1, \dots, a_n together with a set of c_{ij} with the properties (4.1.1) will be called a *normalized frame* for L . The collection of all inverses of a_j in $a_i + a_j$ will be denoted by L_{ij} .

4.2. The mappings $T(i \leftrightarrow k; j \leftrightarrow m)$. Let the a_i and c_{ij} be a fixed normalized frame for L and for i, j, k all different let $P(i \leftrightarrow k; j)$ be the perspective mapping of $L(a_i + a_j)$ onto $L(a_k + a_j)$ determined by the axis c_{ik} . Similarly let $P(i; j \leftrightarrow k)$ be the perspective mapping of $L(a_i + a_j)$ onto $L(a_i + a_k)$ determined by the axis c_{jk} . Then if $n \geq 4$ these perspective mappings have the following property: whenever for $i \neq j$ and $k \neq m$ the product of an ordered sequence of s such perspective mappings is a mapping $T = T(i \leftrightarrow k; j \leftrightarrow m)$ of $L(a_i + a_j)$ onto $L(a_k + a_m)$ with $T(a_i) = a_k$, then T is uniquely determined (such $T(i \leftrightarrow k; j \leftrightarrow m)$ clearly exist; T gives a lattice isomorphism of $L(a_i)$ onto $L(a_k)$, a lattice isomorphism of $L(a_j)$ onto $L(a_m)$ and corresponds c_{ij} with c_{km}).

To verify the general uniqueness of such T it is sufficient to confirm that in the case $i = k$ and $j = m$, T cannot fail to be the identity mapping. If it could, we would choose s to have its least possible value to give such a T different from the identity and derive a contradiction as follows:

Easy calculations, using the modular law, establish the identities:

- (i) $P(i_1 \leftrightarrow i_2; j) P(i_2 \leftrightarrow i_3; j) = P(i_1 \leftrightarrow i_3; j)$,
- (ii) $P(i; j_1 \leftrightarrow j_2) P(i; j_2 \leftrightarrow j_3) = P(i; j_1 \leftrightarrow j_3)$,
- (iii) $P(i \leftrightarrow k; j) P(k; j \leftrightarrow m) = P(i; j \leftrightarrow m) P(i \leftrightarrow k; m)$

if i, j, k, m are all different.

It may therefore be supposed (since s has its least value) that the sequence of mappings which defines T begins:

$$P(i \leftrightarrow t_1; j) P(t_1; j \leftrightarrow t_2) P(t_1 \leftrightarrow t_3; t_2) P(t_3; t_2 \leftrightarrow t_4) \dots \text{(necessarily, } t_1 \neq i, j; t_2 \neq t_1, j).$$

If $t_2 \neq i$ so that i, j, t_1, t_2 are all different, we can, without changing T , replace $P(i \leftrightarrow t_1; j) P(t_1; j \leftrightarrow t_2)$ by $P(i; j \leftrightarrow t_2) P(i \leftrightarrow t_1; t_2)$; then we can

replace $P(i \leftrightarrow t_1; t_2) P(t_1 \leftrightarrow t_3; t_3)$ by $P(i \leftrightarrow t_3; t_2)$. This would express T as a product of fewer than s mappings. Therefore we must have $t_2 = i$.

The same argument shows that $t_3 = j$ and that T is defined by mappings beginning:

$$P(i \leftrightarrow t_1; j) P(t_1; j \leftrightarrow i) P(t_1 \leftrightarrow j; i) P(j; i \leftrightarrow t_4) P(j \leftrightarrow i; t_4) \dots$$

Since $n \geq 4$, there is an integer m such that i, j, t_1, m are all different. Then we may replace $P(t_1; j \leftrightarrow i)$ by $P(t_1; j \leftrightarrow m) P(t_1; m \leftrightarrow i)$; then we may replace $P(i \leftrightarrow t_1; j) P(t_1; j \leftrightarrow m)$ by $P(i; j \leftrightarrow m) P(i \leftrightarrow t_1; m)$; then we may replace $P(t_1; m \leftrightarrow i) P(t_1 \leftrightarrow j; i)$ by $P(t_1 \leftrightarrow j; m) P(j; m \leftrightarrow i)$; then we may replace $P(i \leftrightarrow t_1; m) P(t_1 \leftrightarrow j; m)$ by $P(i \leftrightarrow j; m)$; then we may replace $P(j; m \leftrightarrow i) P(j; i \leftrightarrow t_4)$ by $P(j; m \leftrightarrow t_4)$. T will now be expressed by fewer than s mappings, a contradiction.

This contradiction establishes the uniqueness of $T(i \leftrightarrow k; j \leftrightarrow m)$.

4.3. Fraternal systems and L -numbers. A system of lattice elements $((b)) = ((b_{ij}))$ (it is understood that $i, j = 1, \dots, m$ with $i \neq j$) satisfying $b_{ij} \leq a_i + a_j$ will be called a fraternal system if each $T(i \leftrightarrow k; j \leftrightarrow m)$ maps b_{ij} into b_{km} . Clearly, for given i, j and $x \leq a_i + a_j$ there is one and only one fraternal system $((b))$ with $b_{ij} = x$. Furthermore, if $((b))$ is a fraternal system and $b_{ij} \leq a_i$ for some i, j then this holds for all i, j and b_{ij} is independent of j ; similarly if $b_{ij} \leq a_j$ for some i, j then this holds for all i, j and b_{ij} is independent of i ; finally if b_{ij} is in L_{ij} for some i, j then this holds for all i, j . Fraternal systems $((b))$ with b_{ij} in L_{ij} will be called L -numbers. If β denotes the L -number $((b))$ we write β_{ij} to mean b_{ij} .

We shall develop definitions for addition and multiplication under which the L -numbers will form a regular ring with unit, if $n \geq 4$.

4.4. The addition construction for inverses. A construction, which for fixed i, j applies to two elements x, y in L_{ij} and yields an element z in L_{ij} , is the following: Choose any A, B with the properties:

$$(4.4.1) \quad A(a_i + a_j) = B(a_i + a_j) = 0 = a_i(A + B + a_j), \\ a_i + A + B \geq x.$$

Then define

$$(4.4.2) \quad z = [\{(x + A)(a_i + B) + a_j\}(y + B) + A](a_i + a_j).$$

We shall verify that (i) $za_j = 0$ and (ii) $z + a_j = a_i + a_j$, i.e., z is in L_{ij} .

$$(i) \quad \begin{aligned} za_j &= [\{(x + A)(a_i + B) + a_j\}(y + B) + A]a_j \\ &= [\{(x + A)(a_i + B) + a_j\}(y + B)(A + a_j) + A]a_j \quad (CI) \\ &= [\{(x + A)(a_i + B)(A + a_j) + a_j\}(y + B) + A]a_j \quad (ML) \\ &= [\{(A + x(A + a_j))(a_i + B) + a_j\}(y + B) + A]a_j \quad (ML) \\ &= [\{A(a_i + B) + a_j\}(y + B) + A]a_j \\ &= [(AB + a_j)(y + B) + A]a_j \quad \text{using (4.4.1)} \\ &= [AB + a_j(y + B) + A]a_j \quad (ML) \\ &= [a_j\{y + B(a_i + a_j)\} + A]a_j \quad (CI) \\ &= Aa_j = 0. \end{aligned}$$

$$\begin{aligned}
 \text{(ii)} \quad z + a_j &= [\{(x + A)(a_i + B) + a_j\}(y + B + a_j) + A](a_i + a_j) \\
 &\quad \text{(AL)} \\
 &= [(x + A)(a_i + B) + a_j + A](a_i + a_j) \\
 &= [(x + A)(a_i + B + A) + a_j](a_i + a_j) \quad \text{(AL)} \\
 &= (x + A + a_j)(a_i + a_j) \quad \text{using (4.4.1)} \\
 &= a_i + a_j.
 \end{aligned}$$

4.5. Uniqueness of the addition construction. The z of 4.4 is independent of the A, B used to construct it, at least to this extent: if A_0, B_0 satisfy (4.4.1) then all A, B satisfying (4.4.1) and

$$(4.5.1) \quad (A_0 + B_0 + a_i + a_j)(A + B + a_i + a_j) = a_i + a_j$$

give the same z as A_0, B_0 . It is sufficient to verify that $A_0 + A$ and $B_0 + B$ satisfy (4.4.1) since the z determined by $A_0 + A, B_0 + B$ is \geq the z determined by A_0, B_0 (and \geq the z determined by A, B); the indivisibility of inverses will complete the proof. That $A_0 + A, B_0 + B$ satisfy (4.4.1) is shown as follows:

$$\begin{aligned}
 (A_0 + A)(a_i + a_j) &= [A_0(A + a_i + a_j) + A](a_i + a_j) \quad \text{(CI)} \\
 &= [A_0(a_i + a_j) + A](a_i + a_j) \quad \text{using (4.5.1)} \\
 &= (0 + A)(a_i + a_j) = 0;
 \end{aligned}$$

similarly

$$\begin{aligned}
 (B_0 + B)(a_i + a_j) &= 0 \\
 a_i(A_0 + A + B_0 + B + a_j) &= a_i[(A + B)(A_0 + B_0 + a_i + a_j) \\
 &\quad + A_0 + B_0 + a_j] \quad \text{(CI)} \\
 &= a_i[(A + B)(a_i + a_j) + A_0 + B_0 + a_j] \\
 &\quad \text{using (4.5.1)} \\
 &= a_i[(A + B + a_j)a_i + A_0 + B_0 + a_j] \\
 &\quad \text{(AL), (ML)} \\
 &= a_i(0 + A_0 + B_0 + a_j) = 0; \\
 a_i + A_0 + A + B_0 + B &\geq a_i + A_0 + B_0 \geq x.
 \end{aligned}$$

In particular all $A, B \leq a_i + a_j + a_k$ for some k , give the same z since they give the same z as $A_0 = c_m, B_0 = a_m$ for any m different from i, j, k (such m exist since we assume $n \geq 4$). It follows that for all such $A, B \leq a_i + a_j + a_k$ for some k , the z is independent of the choice of k . From now on we shall restrict A, B to satisfy this additional condition:

$$(4.5.2) \quad A + B \leq a_i + a_j + a_k \quad \text{for some } k.$$

We note that (4.4.1) and (4.5.2) are satisfied by $A = c_{jk}, B = a_k$ if k is different from i, j . For with such A, B ,

$$\begin{aligned}
 A(a_i + a_j) &= c_{jk}(a_j + a_k)(a_i + a_j) = c_{jk}a_j = 0 \\
 B(a_i + a_j) &= a_k(a_i + a_j) = 0 \\
 a_i(A + B + a_j) &= a_i(a_k + a_j) = 0 \\
 a_i + A + B &= a_i + a_j + a_k \geq a_i + a_j \geq x.
 \end{aligned}$$

4.6. The symmetric form for the addition construction. If p, q satisfy

$$(4.6.1) \quad \begin{aligned} a_i + p &= a_i + q = p + q \\ p(a_i + a_j) &= q(a_i + a_j) = 0 \\ p + q &\leq a_i + a_j + a_k \text{ for some } k \end{aligned}$$

then (4.4.1) and (4.5.2) are satisfied by A, B defined by

$$A = (p + x)(q + a_j) \quad B = q,$$

and the z so defined is uniquely determined by x and y . (We note that the conditions (4.6.1) are satisfied by q, p if they are satisfied by p, q ; that $A, B \leq a_i + a_j + a_k$ if $p, q \leq a_i + a_j + a_k$; and that $p = a_k, q = c_{ik}$ do satisfy (4.6.1) if k is different from i, j .) That A, B satisfy (4.4.1) is shown as follows:

$$\begin{aligned} A(a_i + a_j) &= (p + x)[q(a_i + a_j) + a_j] & (ML) \\ &= (p + x)a_j = [p(a_i + a_j) + x]a_j = xa_j = 0; \\ B(a_i + a_j) &= q(a_i + a_j) = 0; \\ a_i(A + B + a_j) &= a_i(A + q + a_j) = a_i(q + a_j) = 0; \\ a_i + A + B &= a_i + (p + q + x)(q + a_j) = (p + q + x)(q + a_j + a_i) \\ &\geq x. & (AL) \end{aligned}$$

Substitution for A, B in (4.4.2) gives

$$\begin{aligned} z &= [\{(p + x)(q + a_j + x)(a_i + q) + a_j\}(y + q) + (p + x)(q + a_j)] \\ &\quad (a_i + a_j) \\ &= [\{(p + x)(p + q) + a_j\}(y + q) + (p + x)(q + a_j)](a_i + a_j) \\ &= [\{(p + x)q + p + a_j\}(y + q) + (p + x)(q + a_j)](a_i + a_j). \end{aligned}$$

Hence

$$(4.6.2) \quad z = [(p + x)(q + a_j) + (q + y)(p + a_j)](a_i + a_j).$$

We shall write $(x \dot{+} y)_{p,q}$ to mean the right side of (4.6.2); we write $x \dot{+} y$ for its value which does not depend on the particular p, q .

4.7. Commutativity of the addition construction. Since $(x \dot{+} y)_{p,q}$ is identical with $(y \dot{+} x)_{q,p}$ it follows that $x \dot{+} y = y \dot{+} x$.

4.8. Associativity of the addition construction. For fixed y in L_{ij} and p, q satisfying (4.6.1) we define:

$$p' = (q + y)(p + a_j) \quad q' = (a_i + p')(q + a_j).$$

Then p', q' also satisfy (4.6.1). To prove this we note the identities:

$$\begin{aligned} a_j + p' &= a_j + p & a_j + q' &= a_j + q \\ y + p' &= y + q & p'q' &= pq. \end{aligned}$$

Now

$$\begin{aligned} a_i + q' &= (a_i + p')(q + a_j + a_i) = a_i + p', \\ p' + q' &= (a_i + p')(q + a_j + p') = a_i + p'. \end{aligned}$$

Hence

$$a_i + q' = a_i + p' = p' + q'.$$

Also

$$\begin{aligned}(a_i + a_j)p' &= (q + y)(0 + a_j) = ya_j = 0, \\ (a_i + a_j)q' &= (a_i + p')(0 + a_j) = (0 + p')a_j = 0\end{aligned}$$

Now if x, w are also in L_{ij} , then

$$(4.8.1) \quad [(x \dot{+} y)_{p,q} \dot{+} w]_{p',q'} = [(w \dot{+} y)_{q',p'} \dot{+} x]_{q,p}$$

which means that $(x \dot{+} y) \dot{+} w = x \dot{+} (y \dot{+} w)$ in virtue of the commutativity of $\dot{+}$.

To prove (4.8.1) we calculate:

$$\begin{aligned}((x \dot{+} y)_{p,q} \dot{+} w)_{p',q'} &= [p' + \{(p + x)(q + a_j) + p'\}(a_i + a_j)](q' + a_j) + (q' + w) \\ &\quad (p' + a_j)(a_i + a_j) \\ &= [\{(p + x)(q + a_j) + p'\}(q + a_j) + (q' + w)(p + a_j)](a_i + a_j) \\ &= [(p + x)(q + a_j) + (q' + w)(p + a_j)](a_i + a_j), \\ [(w \dot{+} y)_{q',p'} \dot{+} x]_{q,p} &= [q + \{(q' + w)(p' + a_j) + (p' + y)(q' + a_j)\}(a_i + a_j)](p + a_j) \\ &\quad + (p + x)(q + a_j)(a_i + a_j) \\ &= [\{(q' + w)(p + a_j) + q\}(a_i + a_j + q)(p + a_j) + (p + x)(q + a_j)] \\ &\quad (a_i + a_j) \\ &= [(q' + w)(p + a_j) + qp + (p + x)(q + a_j)](a_i + a_j) \\ &= [(x \dot{+} y)_{p,q} \dot{+} w]_{p',q'}.\end{aligned}$$

4.9. The addition construction as an operation on L -numbers. If $\alpha = ((x_{ij}))$ and $\beta = ((y_{ij}))$ are L -numbers then $x_{ij} \dot{+} y_{ij} = z_{ij}$ is defined for each $i \neq j$. We shall now verify that $((z_{ij}))$ is an L -number. For this it is sufficient to show that whenever i, j, k are all different:

- (i) $(z_{ij} + c_{jk})(a_i + a_k) = x_{ik} \dot{+} y_{ik},$
- (ii) $(z_{ij} + c_{ik})(a_k + a_j) = x_{kj} \dot{+} y_{kj}.$

To prove (i) choose m so that i, j, k, m are all different and choose $p = a_m, q = c_{im}$. Then

$$\begin{aligned}(z_{ij} + c_{jk})(a_i + a_k) &= [\{(a_m + x_{ij})(c_{im} + a_j) + (c_{im} + y_{ij})(a_m + a_j)\}(a_i + a_j) \\ &\quad + c_{jk}](a_i + a_k) \\ &= [\{(a_m + x_{ij} + c_{jk})(c_{im} + a_j) \\ &\quad + (c_{im} + y_{ij})(a_m + a_j + c_{jk})\}(a_i + a_j + c_{jk}) + c_{jk}](a_i + a_k) \\ &= [(a_m + x_{ij} + c_{jk})(c_{im} + c_{jk} + a_j) \\ &\quad + (c_{im} + y_{ij} + c_{jk})(a_m + a_j + c_{jk})](a_i + a_k) \\ &> [(a_m + x_{ik})(c_{im} + a_k) + (c_{im} + y_{ik})(a_m + a_k)](a_i + a_k).\end{aligned}$$

This shows that $>$ holds in (i). The indivisibility of inverses then implies equality holds in (i).

Similarly,

$$\begin{aligned} (z_{ij} + c_{ik})(a_k + a_j) &= [(a_m + x_{ij} + c_{ik})(c_{im} + c_{ik} + a_j) \\ &\quad + (c_{im} + y_{ij} + c_{ik})(a_m + a_j + c_{ik})](a_k + a_j) \\ &> [(a_m + x_{kj})(c_{km} + a_j) + (c_{km} + y_{kj})(a_m + a_j)](a_k + a_j). \end{aligned}$$

This shows that $>$ (and hence $=$) holds in (ii).

Thus (4.6.2) defines a commutative, associative addition on the L -numbers.

For future reference we write out (4.6.2) with $p = c_{ik}$, $q = a_k$, $x = \alpha_{ij}$, $y = \beta_{ij}$ and $z = (\alpha + \beta)_{ij}$ and (4.4.2) with $A = c_{jk}$, $B = a_k$, $x = \alpha_{ij}$, $y = \beta_{ij}$ and $z = (\alpha + \beta)_{ij}$, thus:

$$(4.9.1) \quad (\alpha + \beta)_{ij} = [\alpha_{kj} + (\beta_{ij} + a_k)(c_{ik} + a_j)](a_i + a_j)$$

$$(4.9.2) \quad (\alpha + \beta)_{ij} = [(\alpha_{ik} + a_j)(\beta_{ij} + a_k) + c_{jk}](a_i + a_j).$$

It is easily verified that the L -number $((x_{ij}))$ with $x_{ij} = a_i$ for all i, j , is a zero for this addition.

We now show that subtraction can be obtained by the formula:

$$(4.9.3) \quad (\alpha - \beta)_{kj} = [\alpha_{ij} + (a_k + \beta_{ij})(a_j + c_{ik})](a_k + a_j).$$

First we verify that the left side of (4.9.3) is in L_{kj} :

$$(\alpha - \beta)_{kj} a_j = [\alpha_{ij} + (a_k + \beta_{ij})(a_j + c_{ik})(a_i + a_j)] a_j \quad (CI)$$

$$= [\alpha_{ij} + (a_k + \beta_{ij}) a_j] a_j = 0;$$

$$(\alpha - \beta)_{kj} + a_j = [a_i + a_j + (a_k + \beta_{ij})(a_j + c_{ik})](a_k + a_j) \quad (AL)$$

$$= [a_i + (a_k + \beta_{ij} + a_j)(a_j + c_{ik})](a_k + a_j) \quad (AL)$$

$$= (a_k + a_i + a_j)(a_i + a_j + c_{ik})(a_k + a_j) \quad (AL)$$

$$= a_k + a_j.$$

Next we verify that (4.9.3) defines an L -number which, when added to β , gives α : using (4.9.1), we obtain

$$\begin{aligned} &[\{ \alpha_{ij} + (a_k + \beta_{ij})(a_j + c_{ik}) \} (a_k + a_j) + (\beta_{ij} + a_k)(c_{ik} + a_j)] (a_i + a_j) \\ &= [\alpha_{ij} + (a_k + \beta_{ij})(a_j + c_{ik})] [a_k + a_j + (\beta_{ij} + a_k)(c_{ik} + a_j)] \\ &\quad (a_i + a_j) \\ &= [\alpha_{ij} + (a_k + \beta_{ij})(a_j + c_{ik})] (a_i + a_j) > \alpha_{ij}. \end{aligned}$$

The indivisibility of inverses then shows that equality holds above. This implies that $(((\alpha - \beta)_{ij}))$ is an L -number and $(\alpha - \beta) + \beta = \alpha$ as stated.

Thus (4.9.1) (equivalently, (4.9.2)) defines an addition under which the L -numbers are an abelian group.

4.10. Multiplication of L -numbers. We shall define the product of L -numbers by the formula:

$$(4.10.1) \quad (\alpha\beta)_{ij} = (\alpha_{ik} + \beta_{kj})(a_i + a_j)$$

using any k different from i, j . We need to verify that $(\alpha\beta)_{ij}$ is in L_{ij} and is independent of k and that $(((\alpha\beta)_{ij}))$ is an L -number.

We have:

$$(\alpha\beta)_{ij}a_j = [\alpha_{ik}(a_j + a_k) + \beta_{kj}]a_j = (0 + \beta_{kj})a_j = 0, \quad (\text{CI})$$

$$(\alpha\beta)_{ij} + a_j = (\alpha_{ik} + a_k + a_j)(a_i + a_j) = a_i + a_j \quad (\text{AL})$$

so that $(\alpha\beta)_{ij}$ is in L_{ij} .

Next, if m is different from i, j, k , then

$$(\alpha_{ik} + \beta_{kj})(a_i + a_j) = (\alpha_{ik} + \beta_{kj} + c_{km})(a_i + a_j) \geq (\alpha_{im} + \beta_{mj})(a_i + a_j) \quad (\text{ST})$$

and hence, by the indivisibility of inverses, equality holds above, showing that $(\alpha\beta)_{ij}$ is independent of k .

To see that $((\alpha\beta)_{ij})$ is a fraternal system (and hence an L -number) we need only verify:

$$(i) \quad ((\alpha\beta)_{ij} + c_{im})(a_m + a_j) = (\alpha\beta)_{mj},$$

$$(ii) \quad ((\alpha\beta)_{ij} + c_{jm})(a_i + a_m) = (\alpha\beta)_{im}.$$

Since $n \geq 4$ we may choose k so that i, j, k, m are all different. Then (i) is proved as follows:

$$((\alpha\beta)_{ij} + c_{im})(a_m + a_j) = [(\alpha_{ik} + \beta_{kj} + c_{im})(a_i + a_j) + c_{im}](a_m + a_j) \quad (\text{ST})$$

$$= (\alpha_{ik} + \beta_{kj} + c_{im})(a_i + a_j + c_{im})(a_m + a_j) \quad (\text{AL})$$

$$= [(\alpha_{ik} + c_{im})(a_m + a_k + a_j) + \beta_{kj}](a_m + a_j) \quad (\text{CI})$$

$$= (\alpha_{mk} + \beta_{kj})(a_m + a_j) = (\alpha\beta)_{mj}.$$

Similarly, (ii) is proved as follows:

$$\begin{aligned} ((\alpha\beta)_{ij} + c_{jm})(a_i + a_m) &= (\alpha_{ik} + \beta_{kj} + c_{jm})(a_i + a_j + c_{jm})(a_i + a_m) \\ &= [\alpha_{ik} + (\beta_{kj} + c_{jm})(a_i + a_m + a_k)](a_i + a_m) \\ &= (\alpha_{ik} + \beta_{km})(a_i + a_m) = (\alpha\beta)_{im}. \end{aligned}$$

It is easily verified that the L -number $((b_{ij}))$ with $b_{ij} = c_{ij}$ for all i, j , is a two-sided unit for this multiplication:

$$(\alpha_{ik} + c_{kj})(a_i + a_j) = \alpha_{ij}; \quad (c_{ik} + \alpha_{kj})(a_i + a_j) = \alpha_{ij}.$$

4.11. Associativity of multiplication. Let α, β, γ be L -numbers and choose i, j, k, m all different. Then

$$((\alpha\beta)\gamma)_{ij} = [(\alpha_{im} + \beta_{mk})(a_i + a_k) + \gamma_{kj}](a_i + a_j) \quad (\text{ST})$$

$$= [(\alpha_{im} + \beta_{mk})(a_i + a_k + a_j) + \gamma_{kj}](a_i + a_j) \quad (\text{AL})$$

$$= (\alpha_{im} + \beta_{mk} + \gamma_{kj})(a_i + a_j)$$

$$= (\alpha(\beta\gamma))_{ij}.$$

This establishes the associativity of the multiplication defined by (4.10.2).

4.12. Distributivity of multiplication and addition. Let α, β, γ be L -numbers and choose i, j, k, m all different. Then, using (4.9.1),

$$\begin{aligned}
 (\alpha\gamma + \beta\gamma)_{ij} &\leq [\alpha_{km} + \gamma_{mj} + (\beta_{im} + \gamma_{mj} + a_k)(a_j + c_{ik} + \gamma_{mj})](a_i + a_j) \\
 &= [\alpha_{km} + (\beta_{im} + a_k)(a_j + c_{ik} + \gamma_{mj}) + \gamma_{mj}](a_i + a_j) \quad (\text{ML}) \\
 &= [\alpha_{km} + (\beta_{im} + a_k)(a_j + c_{ik} + a_m) + \gamma_{mj}](a_i + a_j) \\
 &= [\alpha_{km} + (\beta_{im} + a_k)(a_m + c_{ik}) + \gamma_{mj}](a_i + a_j) \quad (\text{CI}) \\
 &= [(\alpha + \beta)_{im} + \gamma_{mj}](a_i + a_j) = [(\alpha + \beta)\gamma]_{ij}.
 \end{aligned}$$

The indivisibility of inverses now shows that equality holds above and this completes the proof of right distributivity: $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$.

Similarly, using (4.9.2),

$$\begin{aligned}
 (\gamma\alpha + \gamma\beta)_{ij} &\leq [(\gamma_{im} + \alpha_{mk} + a_j)(\gamma_{im} + \beta_{mj} + a_k) + c_{jk}](a_i + a_j) \\
 &= [\gamma_{im} + (\alpha_{mk} + a_j)(\gamma_{im} + \beta_{mj} + a_k) + c_{jk}](a_i + a_j) \quad (\text{ML}) \\
 &= [\gamma_{im} + (\alpha_{mk} + a_j)(\beta_{mj} + a_k) + c_{jk}](a_i + a_j) \quad (\text{CI}) \\
 &= [\gamma_{im} + (\alpha + \beta)_{mj}](a_i + a_j) = [\gamma(\alpha + \beta)]_{ij}.
 \end{aligned}$$

Application of the "indivisibility of inverses" now completes the proof of left distributivity: $\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta$.

4.13. The regular ring of L -numbers. From 4.9, 4.10, 4.11 and 4.12 it follows that under addition and multiplication as defined, the L -numbers form a ring with unit. We call this ring an *auxiliary ring of L* and denote it by \mathfrak{R} .

We shall now show that \mathfrak{R} is a *regular ring*. For this purpose we associate with each α in \mathfrak{R} a fraternal system which we shall call the *reach of α* defined as follows:

$$\text{Reach of } \alpha = ((b)) \text{ with } b_{ij} = (a_i + \alpha_{ij})a_j \text{ for all } i, j.$$

It follows from the isomorphic character of the T -mappings that this does define a fraternal system. Moreover $b_{ij} \leq a_j$ for all i, j (and hence b_{ij} is independent of i) and we write α_j^r for this b_{ij} .

We shall prove:

(4.13.1) For every $b \leq a_j$ and $d = [a_j - b]$ there is an idempotent e in \mathfrak{R} with $e_j^r = b$ and $(1 - e)_j^r = d$.

(4.13.2) For α, β in \mathfrak{R} there is a γ satisfying $\gamma\alpha = \beta$ if and only if $\alpha_j^r \geq \beta_j^r$. From (4.13.1) it will follow that for given α there is an idempotent e with $e_j^r = \alpha_j^r$ and hence from (4.13.2), for suitable β, γ in \mathfrak{R} , $\beta e = \alpha$ and $\gamma\alpha = e$. This implies $\alpha\gamma\alpha = \alpha e = \alpha$ and shows that \mathfrak{R} is a regular ring.

Also, this shows that the correspondence $(\alpha)_i \rightarrow \alpha_j^r$ sets up a $(1, 1)$ order preserving mapping between the lattice of principal left ideals of \mathfrak{R} and the lattice $L(a_j)$.

To prove (4.13.1) set $x = (b + a_i)(d + c_{ij})$. This x is in L_{ij} since:

$$\begin{aligned}
 xa_j &= (b + a_i)(d + c_{ij})a_j = (b + a_i a_j)(d + c_{ij} a_j) \\
 &\qquad\qquad\qquad \text{since } a_j = b + d, \text{ using (ML),} \\
 &= bd = 0,
 \end{aligned}$$

$$\begin{aligned}
 x + a_j &= (b + a_i)(d + c_{ij}) + b + d = (b + a_i + d)(d + c_{ij}) + b \\
 &= (b + a_i + d)(b + d + c_{ij}) = (a_i + a_j)(a_i + a_j) = a_i + a_j.
 \end{aligned}$$

Let e be the L -number with $e_{ij} = x$. Then

$$\begin{aligned}
 (ee)_{ij} &\leq [(b + a_i)(d + c_{ij}) + c_{jk}](a_i + a_k + b) \\
 &\quad + [(b + a_i)(d + c_{ij}) + c_{ik}](a_k + a_j)(a_i + a_j) \\
 &= (b + a_i)(d + c_{ij}) + (c_{jk}(a_i + a_k + b) \\
 &\quad + [(b + a_i)(d + c_{ij}) + c_{ik}](a_k + a_j)(a_i + a_j)) \\
 &= (b + a_i)(d + c_{ij}) + (b + a_i + a_k)[c_{jk} + (b + a_i)(d + c_{ij}) \\
 &\quad + c_{ik}]a_j \\
 &\leq (b + a_i)(d + c_{ij}) + b[c_{ik} + d + c_{ij}](a_i + a_j) \\
 &= (b + a_i)(d + c_{ij}) = e_{ij}
 \end{aligned}$$

The indivisibility of inverses shows that equality holds above and hence this e is idempotent.

Finally

$$e_j^r = [(b + a_i)(d + c_{ij}) + a_i]a_j = [(b + a_i)(a_i + a_j)]a_j = b;$$

since (4.9.3) shows that

$$(1 - e)_{kj} = [c_{ij} + (a_k + e_{ij})(a_j + c_{ik})](a_k + a_j),$$

it follows that

$$\begin{aligned}
 (1 - e)_j^r &= [c_{ij} + (a_k + e_{ij})(a_j + c_{ik}) + a_k]a_j \\
 &= [c_{ij} + (a_k + e_{ij})(a_j + a_k + c_{ik})]a_j \\
 &= [c_{ij} + a_k + e_{ij}]a_j = [c_{ij} + e_{ij}]a_j \\
 &= [c_{ij} + (b + a_i)(d + c_{ij})]a_j \\
 &= [d + c_{ij}]a_j = d.
 \end{aligned}$$

This completes the proof of (4.13.1).

(4.13.2) may be proved as follows: $\gamma\alpha = \beta$ means

$$(\gamma_{ij} + \alpha_{jk})(a_i + a_k) = \beta_{ik}$$

and because of the indivisibility of inverses, this is equivalent to:

$$(4.13.3) \quad (\gamma_{ij} + \alpha_{jk})(a_i + a_k) \leq \beta_{ik}.$$

This condition is equivalent to

$$(4.13.4) \quad (\gamma_{ij} + \alpha_{jk})(a_i + a_k) + \alpha_{jk} \leq \beta_{ik} + \alpha_{jk}$$

(clip both sides of (4.13.4) by $(a_i + a_k)$ to derive (4.13.3)).

Now (4.13.4) is equivalent to

$$\gamma_{ij} + \alpha_{jk} \leq \beta_{ik} + \alpha_{jk}$$

and hence to

$$\gamma_{ij} \leq (\beta_{ik} + \alpha_{jk})(a_i + a_j).$$

Thus $\gamma\alpha = \beta$ for some γ in \mathfrak{R} if and only if $(\beta_{ik} + \alpha_{jk})(a_i + a_j) \geq$ some x in L_{ij} . This is equivalent to:

$$(4.13.5) \quad (\beta_{ik} + \alpha_{jk})(a_i + a_j) + a_j = a_i + a_j$$

(if (4.13.5) holds, x may be chosen

$$= [(\beta_{ik} + \alpha_{jk})(a_i + a_j) - (\beta_{ik} + \alpha_{jk})a_j].$$

Thus $\gamma\alpha = \beta$ for some γ in \mathfrak{R} if and only if

$$\beta_{ik} + \alpha_{jk} + a_j \geq a_i + a_j \quad (\text{ML})$$

i.e.,

$$(4.13.6) \quad \beta_{ik} + \alpha_{jk} + a_j \geq a_i + \beta_{ik}.$$

Now (4.13.6) is equivalent to

$$(4.13.7) \quad (\beta_{ik} + \alpha_{jk} + a_j)(a_j + a_k) \geq (a_i + \beta_{ik})(a_j + a_k).$$

(add β_{ik} to both sides of (4.13.7) to derive (4.13.6)), hence to

$$\alpha_{jk} + a_j \geq (a_i + \beta_{ik})a_k$$

and finally to

$$(\alpha_{jk} + a_j)a_k \geq (a_i + \beta_{ik})a_k$$

i.e.,

$$\alpha_j' \geq \beta_j'.$$

which is equivalent to (4.13.2).

We note that $0_j' = (a_i + a_i)a_j = 0$ and hence, using (4.13.2), $\alpha_j' = 0$ if and only if $\alpha = 0$.

We note also:

(4.13.8) The idempotent e in (4.13.1) is unique.

For if e, f are idempotents with $e_j' = f_j'$ and $(1 - e)_j' = (1 - f)_j'$ then (4.13.2) shows that $ef = e$ and $(1 - e)(1 - f) = 1 - e$, i.e., $ef = e$ and $f = ef$ so that $e = f$.

This completes the proof that \mathfrak{R} is a regular ring. In Part II of this note, to be published separately, the proof of the coordinatization theorem will be completed.

REFERENCES

1. J. von Neumann, *Continuous Geometry* (Princeton, N.J.: Institute for Advanced Study, 1936), vol. I.
2. J. von Neumann, *Continuous Geometry* (Princeton, N.J.: Institute for Advanced Study, 1936), vol. II.

An Inequality of Steinitz and the Limits of Riemann Sums

ISRAEL HALPERIN, F.R.S.C. and NORMAN MILLER

1. Introduction. Consider a function $F(t)$ defined for $0 \leq t \leq 1$ with values in a linear normed vector space V and suppose that $F(t)$ is bounded, i.e., for some $k < \infty$, $\|F(t)\| \leq k$ for all t .

For every subdivision of the interval $(0, 1)$

$$D: \quad 0 = t_0 < t_1 < \dots < t_j = 1 \quad j = 1, 2, \dots$$

and for every choice of intermediary values

$$E: \quad \xi_1, \xi_2, \dots, \xi_j \text{ with } t_{i-1} \leq \xi_i < t_i, \quad i = 1, \dots, j,$$

let $\Delta(D) = \max(t_i - t_{i-1})$, $i = 1, \dots, j$ and let $\sum(D, E)$ denote the Riemann sum

$$\sum_{i=1}^j F(\xi_i)(t_i - t_{i-1}).$$

A vector v will be called a *Riemann limit* of F if $\|\sum(D_n, E_n) - v\| \rightarrow 0$ as $n \rightarrow \infty$ for some suitable sequence of Riemann sums $\sum(D_n, E_n)$ for which $\Delta(D_n) \rightarrow 0$ as $n \rightarrow \infty$. The set of all Riemann limits of F will be denoted by S . It is easy to see that S is a closed set.

It was shown by P. Hartman (1) and by R. L. Jeffery (3), using different methods of proof, that S is a *convex* set if V is finite dimensional. Hartman's proof is based on a vector inequality (this inequality had actually been established previously by E. Steinitz (4)) while Jeffery's proof depends on a theorem of Helly (2) and the fundamental theorem of the Lebesgue calculus.

In this note we give a simple proof of a sharpened form of the Steinitz inequality and use it to show that S is convex if V is real or complex Euclidean (i.e., an inner product space) of *arbitrary* dimension.

2. The Steinitz inequality. Suppose $v_i = Q_0 Q_i$, $i = 1, \dots, m$ are vectors in a real N dimensional vector space (a complex vector space may always be considered as a real vector space of twice the original dimension) and suppose P is a point of the parallelepiped (possibly degenerate) determined by the v_i , i.e., $Q_0 P = t_1 v_1 + \dots + t_m v_m$ with $0 \leq t_i \leq 1$ for each i . Call Q a *vertex* of the parallelepiped if $Q_0 Q = c_1 v_1 + \dots + c_m v_m$ with $c_i = 0$ or 1 for each i .

Steinitz (4, p. 170) showed that if $\|v_i\| \leq k$ for each i then for at least one vertex Q ,

$$(2.1) \quad \|PQ\| \leq Nk.$$

His argument was the following:

(i) It may be supposed that the v_i are linearly independent and hence that $m < N$. For if $v_m = r_1 v_1 + \dots + r_{m-1} v_{m-1}$, then $Q_0 P = (t_1 + r r_1) v_1 + \dots + (t_{m-1} + r r_{m-1}) v_{m-1} + (t_m - r) v_m$ for every real number r ; when r increases continuously from zero there is a least r for which one of these new coefficients becomes zero or one and so reduces the problem to the case of $m - 1$ vectors v_i .

(ii) By the triangle inequality: $\|t_1 v_1 + \dots + t_m v_m\| \leq mk$.

If, in (ii), we use the vertex Q for which $c_i = 0$ if $t_i \leq \frac{1}{2}$ and $c_i = 1$ if $t_i > \frac{1}{2}$, it is clear that (2.1) will hold with $\frac{1}{2} Nk$ in place of Nk . Moreover the argument of Steinitz shows that with this constant the inequality is valid in a real dimensional vector space with *arbitrary* norm; simple examples show that for arbitrary norm $\frac{1}{2} Nk$ is the best possible constant.

If the vector space is real Euclidean, the inequality (2.1) is valid, as stated by Steinitz (and Hartman) without proof, with $\frac{1}{2} \sqrt{Nk}$ in place of Nk . We prove this by induction on N , as follows.

We may clearly suppose as in (i) that the v_i are linearly independent and that $N = m$. Let PP' be a perpendicular of shortest length from P to an $m - 1$ dimensional flat containing an $m - 1$ dimensional face of the parallelepiped. Clearly P' must be a *boundary* or *interior* point of the face and PP' is perpendicular to $P'Q$ for every Q in the $m - 1$ flat; hence, by induction, $\|PQ\| \leq \frac{1}{2} \sqrt{Nk}$ for some vertex Q .

This argument actually shows (both for real and complex Euclidean spaces) that for some vertex Q ,

$$\|PQ\| \leq \frac{1}{2} \max (\|v_1\|^2 + \dots + \|v_m\|^2)^{\frac{1}{2}}$$

for all linearly independent subsets of vectors from the v_1, \dots, v_m . In particular,

$$(2.2) \quad \|PQ\| \leq \frac{1}{2} \left(\sum_{i=1}^m \|v_i\|^2 \right)^{\frac{1}{2}}.$$

An inequality for σ , the root mean square of $\|PQ\|$ when Q varies over all 2^m vertices of the parallelepiped, can be obtained as follows. From the formula

$$\|x_1 v_1 + \dots + x_m v_m\|^2 = \sum_{i,j=1}^m x_i x_j (v_i, v_j)$$

where the bracket indicates inner product, with each x_i independently taking the values t_i and $1 - t_i$, we obtain:

$$2^m \sigma^2 = 2^{m-1} \sum_{i=1}^m (t_i^2 + (1 - t_i)^2) (v_i, v_i) + 2^{m-2} \sum_{i \neq j} (v_i, v_j),$$

hence

$$4\sigma^2 = \left\| \sum_{i=1}^m v_i \right\|^2 + 4 \sum_{i=1}^m (t_i - \frac{1}{2})^2 \|v_i\|^2,$$

$$\sigma \leq \frac{m}{2} \left(1 + \frac{1}{m} \right)^{\frac{1}{2}} k < \frac{k}{2} (m + \frac{1}{2}).$$

3. The convexity of S when V is Euclidean. Suppose P_1 and P_2 are points of S and suppose P is a point on the line segment joining P_1 and P_2 . Let $\epsilon > 0$ be a fixed number. Then there are Riemann sums $\sum(D_1, E_1)$, $\sum(D_2, E_2)$ such that

$$\|\sum(D_1, E_1) - P_1\| < \epsilon, \quad \|\sum(D_2, E_2) - P_2\| < \epsilon$$

and we may even suppose that each point t_{i1} , $i = 0, 1, \dots, j$, of D_1 is also one of the points $t_{h(i),2}$ of D_2 . Put

$$X_i = F(\xi_{i1})(t_{i1} - t_{i-1,1}) \quad i = 1, 2, \dots, j$$

and

$$Y_i = \sum_{q=h(i-1)+1}^{h(i)} F(\xi_{q2})(t_{q2} - t_{q-1,2}) \quad i = 1, 2, \dots, j.$$

Let

$$Q_0 = \sum_{i=1}^j X_i$$

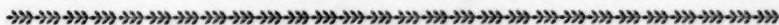
and $v_i = Y_i - X_i$ so that $\|v_i\| \leq 2k(t_i - t_{i-1})$ for all $i = 1, 2, \dots, j$. It follows from (2.2) that for some Riemann sum $\sum(D, E)$ with $\Delta(D) < \Delta(D_1)$,

$$\begin{aligned} \|\sum(D, E) - P\| &< \epsilon + \frac{2k}{2} \left(\sum_{i=1}^j (t_i - t_{i-1})^2 \right)^{\frac{1}{2}} \\ &< \epsilon + k \left(\sum_{i=1}^j (t_i - t_{i-1}) \Delta(D_1) \right)^{\frac{1}{2}} \\ &= \epsilon + k(\Delta(D_1))^{\frac{1}{2}} \end{aligned}$$

which is arbitrarily small if ϵ and $\Delta(D_1)$ are sufficiently small. This shows that S is a convex set if V is real (or complex) Euclidean of arbitrary dimension.

REFERENCES

1. P. Hartman, *On the limits of Riemann approximating sums*, Quarterly J. Math., 18 (1947), 124-127.
2. E. Helly, *Ueber lineare Funktionaloperationen*, S. B. Akad. Wiss. Wien (IIa), 121, (1912), 283.
3. R. L. Jeffery, *Limit points of Riemann sums*, Trans. Royal Soc. of Canada, Series III, 44 (1950), Sec. III, 43-49.
4. E. Steinitz, *Bedingt konvergente Reihen und konvexe Systeme*, J. reine angew. Math., 143 (1913), 128-175.



On an Array of Aitkin

LEO MOSER and MAX WYMAN, F.R.S.C.

1. Introduction. Let G_n denote the number of ways in which n distinguishable objects can be placed into an unrestricted number of indistinguishable boxes. The numbers G_n have been the object of numerous investigations. A recent thesis of H. Finlayson (6) on this topic lists over fifty references, and in almost all cases the references we supply are by no means the only ones which contain the required results. The following are some of the principle results concerning the G 's.

$$(1.1) \quad \sum_{n=0}^{\infty} G_n \frac{x^n}{n!} = e^{e^x - 1}.$$

$$(1.2) \quad G_{n+1} = (G + 1)^n, \quad G_0 = G_1 = 1. *$$

$$(1.3) \quad G_n = \frac{1}{e} \sum_{r=0}^{\infty} \frac{r^n}{r!}.$$

$$(1.4) \quad G_p \equiv 2 \pmod{p}. **$$

$$(1.5) \quad G_{p+n} \equiv G_n + G_{n+1} \pmod{p}.$$

These results are proved by G. T. Williams (10) though they were all discovered by earlier authors. The following representation of G_n as a finite sum is given by E. T. Bell:

$$(1.6) \quad G_n = \left(\frac{\Delta}{1!} + \frac{\Delta^2}{2!} + \dots + \frac{\Delta^n}{n!} \right) 0^n = \sum_{r=1}^n \sigma_n^r.$$

The notations here is that of finite differences. The numbers

$$\frac{\Delta^r 0^n}{r!} = \sigma_n^r$$

are known as divided differences of zero, or alternatively as Stirling numbers of the second kind. Explicitly

$$(1.7) \quad \sigma_n^r = \frac{(-1)^r}{r!} \sum_{i=1}^r \left[(-1)^i \binom{r}{i} i^n \right].$$

Many properties of these numbers are developed by C. Jordan (7). The most extensive published tables of σ_n^r seem to be those of A. Cayley (5) but these have been extended in (6).

*Here and elsewhere we use the standard symbolic notation in which a "polynomial" $A_0 + A_1 G + A_2 G^2 + \dots + A_n G^n$ is to be interpreted as $A_0 + A_1 G_1 + A_2 G_2 + \dots + A_n G_n$.

**Throughout the paper, p is used to denote a prime.

One of the most elegant defining properties of the G 's is

$$(1.8) \quad \Delta^n G_1 = G_n, \quad G_0 = G_1 = 1.$$

To compute G_n , A. C. Aitkin (1) used an algorithm based on (1.8). He considered the following array:

$m \backslash n$	0	1	2	3	4	5	6...
0	1	1	2	5	15	52	203
1	2	3	7	20	67		
2	5	10	27	87			
3	15	37	114				
4	52	151					
5	203						
:							

If we denote the number in the m th row and n th column by $G_{m,n}$, then the array is determined by:

$$(1.9) \quad G_{m,n} = G_{m-1,n+1} + G_{m-1,n} \quad (m \geq 1),$$

$$(1.10) \quad G_{0,n+1} = G_{n,0}$$

$$(1.11) \quad G_{0,0} = G_{0,1} = 1.$$

From (1.8) or (1.2) it follows that

$$(1.12) \quad G_{0,n} = G_n.$$

This array was rediscovered by H. W. Becker (2) who used it to find

$$\begin{aligned} G_{25} &= && 4, & 638, & 590, & 332, & 229, & 999, & 353 \\ G_{30} &= && 846, & 749, & 014, & 511, & 809, & 332, & 450, & 147 \\ G_{35} &= & 286, & 600, & 203, & 019, & 560, & 266, & 563, & 340, & 426, & 570. \end{aligned}$$

The same array was rediscovered by F. Westick (9) who noted its utility in summing the series in (1.3). In this note we discuss some properties of the non-border elements of the array, and consider a more general array.

2. The numbers $G_{m,n}$. We first prove

THEOREM 1.

$$G_{m,n} = (G+1)^m G^n.$$

Proof. Let E be the advancing operator

$$E(G_n) = G_{n+1}$$

and

$$E(G_{m,n}) = G_{m,n+1}.$$

From (1.9) we have

$$G_{m,n} = (E+1) G_{m-1,n} = \dots = (E+1)^m G_{0,n} = (E+1)^m G_n = (G+1)^m G^n.$$

The analogue of (1.3) is given by

THEOREM 2.

$$G_{m,n} = \frac{1}{e} \sum_{r=0}^{\infty} (r+1)^m \frac{r^n}{r!}$$

Proof. By (1.3) and Theorem 1,

$$\frac{1}{e} \sum_{r=0}^{\infty} (r+1)^m \frac{r^n}{r!} = \frac{1}{e} \sum_{i=0}^m \binom{m}{i} \sum_{r=0}^{\infty} \frac{r^{n+i}}{r!} = (G+1)^m G^n = G_{m,n}.$$

An alternative proof is easily obtained by showing that the expression on the right in Theorem 2 satisfies the conditions (1.9) to (1.11).

The following congruence is implicit in some earlier papers.

THEOREM 3.

$$G_{n+mp} = G_{m,n} \pmod{p}.$$

Proof. The theorem is trivial for $m = 0$. Proceed by induction over m and using (1.5) we have:

$$G_{n+(m+1)p} \equiv G_{n+mp} + G_{n+1+mp} \equiv G_{m,n} + G_{m,n+1} = G_{m+1,n} \pmod{p}.$$

3. The generalized array. Let a and b be real or complex numbers. We consider the following array:

$m \backslash n$	0	1	2	3	4	5	6
0	a	b	$a+b$	$2a+3b$	$6a+9b$	$21a+31b$	$82a+121b...$
1	$a+b$	$a+2b$	$3a+4b$	$8a+12b$	$27a+40b$		
2	$2a+3b$	$4a+6b$	$11a+16b$	$35a+52b$			
3	$6a+9b$	$15a+22b$	$46a+68b$				
4	$21a+31b$	$61a+90b$					
5	$82a+121b$						
:							

If we denote the number in the m th row and n th column by $A_{m,n}$ then the array is determined by:

$$(3.1) \quad A_{m,n} = A_{m-1,n+1} + A_{m-1,n} \quad (m \geq 1)$$

$$(3.2) \quad A_{0,n+1} = A_{n,0}$$

and

$$(3.3) \quad A_{0,0} = a, \quad A_{0,1} = b.$$

The case $a = b = 1$ yields $G_{m,n}$. Define

$$(3.4) \quad A_n = A_{0,n}.$$

Exactly as for the G 's we obtain

THEOREM 4.

$$A_{m,n} = (A+1)^m A^n.$$

We proceed to obtain a generating function for A_n . Let

$$(3.5) \quad F = F(x, y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} A_{m,n} \frac{x^m y^n}{m! n!}.$$

Differentiating (3.5) and using (3.1) yields

$$(3.6) \quad \frac{\partial F}{\partial x} = F + \frac{\partial F}{\partial y}.$$

The general solution of (3.6) is

$$(3.7) \quad F(x, y) = e^x f(x + y).$$

Where the form of f is to be determined by (3.2) and (3.3). Using these, as well as (3.5) and (3.6) we have

$$(3.8) \quad \begin{aligned} F(x, 0) &= \sum_{m=0}^{\infty} A_{m,0} \frac{x^m}{m!} = a + \sum_{m=1}^{\infty} A_{m,0} \frac{x^m}{m!} \\ &= a + \frac{d}{dx} \left[\sum_{m=2}^{\infty} A_{0,m} \frac{x^m}{m!} \right] = a + \frac{d}{dx} [F(0, x) - a - bx] \\ &= a - b + \frac{d}{dx} \{F(0, x)\}. \end{aligned}$$

From (3.7) and (3.8) we obtain

$$(3.9) \quad \frac{df}{dx} = e^x f + (b - a).$$

Now (3.9) is a linear differential equation whose solution, satisfying $f(0) = F(0, 0) = a$, is given by

$$(3.10) \quad f(x) = ae^{e^x-1} + (b-a)e^{e^x} \int_0^x e^{-e^t} dt.$$

Note that the case $a = b = 1$ of this result yields an independent proof of (1.1). In view of Theorems 4 and (3.10) and the fact that the $G_{m,n}$ have already been studied, the theory of the general array is reduced to the case $a = 0, b = 1$. In this case the array is:

$m \backslash n$	0	1	2	3	4	5	6...
0	0	1	1	3	9	31	121
1	1	2	4	12	40		
2	3	6	16	52			
3	9	22	68				
4	31	90					
5	121						

Let the number in the m th row and n th column be denoted by $B_{m,n}$ and let $B_{0,n} = B_n$. From (3.10) or directly, we have

$$(3.11) \quad A_n = aG_n + (b-a)B_n.$$

Also from (3.10)

$$(3.12) \quad \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x} \int_0^x e^{-e^t} dt.$$

We now prove the analogue of (1.2)

THEOREM 5.

$$B_{n+1} = (B + 1)^n - 1, \quad B_0 = 0, \quad B_1 = 1.$$

Proof. Let

$$(3.13) \quad \psi(x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

By (3.9) we know that ψ satisfies

$$(3.14) \quad \frac{d\psi}{dx} = e^x \psi + 1.$$

Differentiating (3.14) n times yields

$$(3.15) \quad \frac{d^{n+1}\psi}{dx^{n+1}} = \sum_{r=0}^n \binom{n}{r} \frac{d^r \psi}{dx^r} \cdot e^x.$$

Setting $x = 0$ in (3.15) and using (3.13) gives

$$(3.16) \quad B_{n+1} = \sum_{r=0}^n \binom{n}{r} B_r,$$

which is a form of the required result. We note that (3.16) holds also for the G 's, the difference in the symbolic forms being accounted for by the fact that $G_0 = 1$ while $B_0 = 0$.

Other properties of the B 's seem to be more complicated than the corresponding properties of the G 's. In order to obtain an explicit representation of B_n as a finite sum we must first consider a set of polynomials defined by

$$(3.17) \quad \sum_{n=0}^{\infty} G_n(z) \frac{x^n}{n!} = e^{z(e^x-1)}.$$

These polynomials and some generalizations of them have been studied by I. Schwatt (8), E. T. Bell (3) and H. Burger (4) among others. Clearly

$$(3.18) \quad G_n = G_n(1).$$

We list several interesting properties of the $G_n(z)$. These are proved in the papers mentioned above, but only (3.19) will be used in what follows.

$$(3.19) \quad G_n(z) = \sum_{r=1}^n \sigma_r z^r, \quad (n > 0), \quad G_0(z) = 1.$$

$$(3.20) \quad G_n(z) = e^{-z} \sum_{r=0}^{\infty} \frac{r^n z^r}{r!}.$$

$$(3.21) \quad G_n(z) = e^{-z} \left(z \frac{d}{dz} \right)^n e^z.$$

$$(3.22) \quad G_{n+1}(z) = z \left[G_n(z) + \frac{d}{dz} G_n(z) \right].$$

$$(3.23) \quad G_n(x+y) = \left(G(x) + G(y) \right)^n.$$

We now prove the following analogue of (1.6).

THEOREM 6.

$$B_n = \sum_{r=1}^n \sigma_n^r (0! - 1! + 2! \dots (-1)^{r-1} (r-1)!)$$

Proof. From (3.12) we have

$$(3.24) \quad \sum_{n=0}^{\infty} \frac{B_n x^n}{n!} = e^{e^x} \left[\int_0^{\infty} e^{-e^t} dt - \int_x^{\infty} e^{-e^t} dt \right].$$

Let $e^t = v + 1$ in the first integral and $e^t = (v + 1)e^x$ in the second. In either case the new limits are 0 and ∞ and the dt is replaced by $dv/(v + 1)$. Hence, the

$$(3.25) \quad \begin{aligned} \sum_{n=0}^{\infty} \frac{B_n x^n}{n!} &= e^{e^x} \int_0^{\infty} \left[e^{-(v+1)} - e^{-(v+1)e^x} \right] \frac{dv}{v+1} \\ &= \int_0^{\infty} \left(e^{e^x-1} - e^{-v(e^x-1)} \right) \frac{e^{-v}}{v+1} dv. \end{aligned}$$

Now using (3.17) and equating coefficients of x^n yields

$$(3.26) \quad B_n = \int_0^{\infty} \left[G_n(1) - G_n(-v) \right] \frac{e^{-v}}{v+1} dv.$$

From (3.26) and (3.19) we have

$$\begin{aligned} B_n &= \sum_{r=1}^n \sigma_n^r \int_0^{\infty} \frac{e^{-v}}{v+1} (1 - (-v)^r) dv \\ &= \sum_{r=1}^n \sigma_n^r \int_0^{\infty} e^{-v} \left(1 - v + v^2 \dots (-1)^{r-1} v^{r-1} \right) dv \\ &= \sum_{r=1}^n \sigma_n^r (0! - 1! + 2! \dots (-1)^{r-1} (r-1)!). \end{aligned}$$

4. Congruence property of B_p . We conclude with the following analogue of (1.4),

THEOREM 7.

$$B_p \equiv - \left(\frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{(p-1)!} \right) \pmod{p}$$

Proof. It is easy to see and proved in (1) that

$$(4.1) \quad \sigma_p^r \equiv 0 \pmod{p} \quad (1 < r < p).$$

Hence from Theorem 6 and (4.1) we obtain

$$(4.2) \quad B_p \equiv 1 + \left(0! - 1! + 2! \dots - (p-2)! + (p-1)! \right) \pmod{p}, \quad p > 2.$$

By Wilson's theorem

$$(4.3) \quad (p-1)! \equiv -1 \pmod{p}$$

and

$$(4.4) \quad (P-r)! \equiv \frac{(-1)^r}{(r-1)!} \pmod{p}.$$

Now (4.4) and (4.2) yield the required result.

REFERENCES

1. A. C. Aitkin, *A problem on combinations*, Math. Notes Edinburgh, *21* (1933), 18-23.
2. H. W. Becker, *Solution to problem*, Amer. Math. Monthly, *48* (1941), 701-702.
3. E. T. Bell, *Exponential polynomials*, Ann. Math., *35* (1934), 258-277.
4. H. Burger, *Problem 138*, Elemente der Math., *7* (1952), 136-137.
5. A. Cayley, *Tables of $\Delta^n 0^n/m!$ up to $m = n = 20$* , Trans. Camb. Phil. Soc., *13* (1883), 1-4.
6. H. Finlayson, *Numbers generated by $e^{e^x}-1$* , Master's thesis, University of Alberta (1954). Unpublished.
7. C. Jordan, *Calculus of finite differences* (Chelsea, N.Y., 1947).
8. I. Schwatt, *An introduction to operations with infinite series* (University of Pennsylvania Press, 1924).
9. F. Westick, *Note 2256*, Math. Gaz., *35* (1951), 261.
10. G. T. Williams, *Numbers generated by $e^{e^x}-1$* , Amer. Math. Monthly, *52* (1945), 323-327.



On Ordered, Finitely Generated, Solvable Groups

By RIMHAK REE

Presented by R. L. JEFFERY, F.R.S.C.

1. In this note we consider ordered, finitely generated, solvable groups. Our main result is as follows: If an ordered, finitely generated, solvable group \mathfrak{G} satisfies the maximal condition for subgroups¹ then \mathfrak{G} is nilpotent. We also show that if a finitely generated ordered group \mathfrak{G} satisfies the maximal condition for subgroups then \mathfrak{G} is nilpotent in a generalized sense. However, if \mathfrak{G} does not satisfy the maximal condition for subgroups then \mathfrak{G} is not necessarily nilpotent, for we prove in §4 that $\mathfrak{F}/\mathfrak{F}''$ can be ordered, where \mathfrak{F} is the free group generated by a finite (or even countably infinite) number of free generators, and \mathfrak{F}'' denotes the second derived group of \mathfrak{F} .

2. We recall some properties of ordered groups, established for the most part by F. W. Levi (6) and K. Iwasawa (3), which we shall need later.

Let \mathfrak{G} be an ordered group, which we write multiplicatively. The absolute value $|A|$ of $A \in \mathfrak{G}$ is defined by $|A| = A$ if $A \geq 1$ and $|A| = A^{-1}$ if $A \leq 1$.

For given $A, B \in \mathfrak{G}$, if $|A|^n < |B|$ for all positive integers n , then $|A|$ is said to be *infinitely small* to $|B|$, and this statement is denoted by $|A| \ll |B|$. The relation \ll is transitive.

If $|A|$ is neither infinitely small to $|B|$ nor $|B|$ is infinitely small to $|A|$ then A and B are said to be *comparable*, and we write $A \sim B$. Comparability is an equivalence relation and therefore defines equivalence classes in \mathfrak{G} , which we shall call *C-classes*. The unit 1 of \mathfrak{G} forms a C-class by itself. Let \mathfrak{C} be the set of all C-classes different from the unit class.

If λ and μ are two different C-classes then either $|X| \ll |Y|$ for all $X \in \lambda$ and all $Y \in \mu$ or $|X| \gg |Y|$ for all $X \in \lambda$ and all $Y \in \mu$. We define a linear order in L as follows: If $\lambda, \mu \in \mathfrak{C}$, then $\lambda < \mu$ if $X \ll Y$ for all $X \in \lambda, Y \in \mu$.

Let λ be any C-class in L , and put $G_\lambda = U\{\mu | \mu \ll \lambda\}$, $G_\lambda^* = U\{\mu | \mu < \lambda\}$. Then G_λ and G_λ^* are subgroups of \mathfrak{G} , and G_λ^* is normal in G_λ . Since $|A'| \leq |A|$ and $A \in G_\lambda^*$ imply $A' \in G_\lambda^*$, we can define a linear order in G_λ/G_λ^* so that G_λ/G_λ^* becomes an ordered group and so that the natural homomorphism from G_λ to G_λ/G_λ^* is order-preserving. The order in $\mathfrak{R}_\lambda = G_\lambda/G_\lambda^*$ defined above is Archimedian, and \mathfrak{R}_λ is order-isomorphic to a subgroup of the additive group of real numbers.

¹Finitely generated solvable groups which satisfy the maximal condition for subgroups have been investigated by K. A. Hirsch, and were called by him "S-groups." Cf. (2).

Let X be an arbitrary fixed element in \mathfrak{G} . Then for any C -class λ , $\lambda' = X^{-1}\lambda X$ is also a C -class, and the mapping $\lambda \rightarrow \lambda'$ is a one-to-one order-preserving mapping of \mathfrak{L} onto itself. The mapping $Y \rightarrow X^{-1}YX$ induces an order-preserving isomorphism of \mathfrak{R}_λ and $\mathfrak{R}_{\lambda'}$.

If \mathfrak{L} admits no order-preserving mapping of \mathfrak{L} onto itself, except the identity mapping, as is the case when the linear ordering in \mathfrak{L} is a well-ordering or an inverse well-ordering, then every \mathfrak{G}_λ and \mathfrak{G}_λ^* is normal in \mathfrak{G} , and so \mathfrak{G} is solvable in a generalized sense. If, furthermore, every \mathfrak{R}_λ admits no order-preserving automorphism except the identity, as is the case when every \mathfrak{R}_λ is order-isomorphic to the additive group of integers, then $[\mathfrak{G}, \mathfrak{G}_\lambda] \subseteq \mathfrak{G}_\lambda^*$, and so \mathfrak{G} is nilpotent in a generalized sense.

3. THEOREM 1. *If an ordered group \mathfrak{G} satisfies the maximal condition for subgroups, then \mathfrak{G} is nilpotent in a generalized sense. In fact, \mathfrak{G} is a ZD-group (cf. 5), i.e., a group with a descending central series.*

Proof. Since \mathfrak{G} satisfies the maximal condition for subgroups, \mathfrak{L} is well-ordered, and every \mathfrak{R}_λ is finitely generated, since \mathfrak{G}_λ is finitely generated. Since every finitely generated subgroup of the additive group of real numbers is isomorphic to the additive group of integers, every \mathfrak{R}_λ is order-isomorphic to the additive group of integers. Thus we know by the last remark in (2) above that $\{\mathfrak{G}_\lambda\}$ is a descending central series.

THEOREM 2.² *An ordered, finitely generated, solvable group \mathfrak{G} is nilpotent if and only if \mathfrak{G} satisfies the maximal condition for subgroups.*

Proof. Suppose first that \mathfrak{G} satisfies the maximal condition for subgroups. Then as in the proof of Theorem 1 every \mathfrak{R}_λ is order-isomorphic to the additive group of integers.

We shall show that the number of C -classes in \mathfrak{L} is finite. Let the derived series of \mathfrak{G} be

$$\mathfrak{G} = \mathfrak{G}^{(0)} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset \dots \supset \mathfrak{G}^{(t)} = 1,$$

where $\mathfrak{G}^{(k)} = (\mathfrak{G}^{(k-1)}, \mathfrak{G}^{(k-1)})$ as usual. We proceed by complete induction with respect to t . If $t = 0$ then \mathfrak{G} is the unit group, and so \mathfrak{L} is empty. Assume that the number of C -classes in \mathfrak{G}' is finite. Let $\mathfrak{G}/\mathfrak{G}'$ be generated by r elements. If there were an infinite number of C -classes in \mathfrak{G} , then, no matter how large r is, we would be able to choose $r + 1$ elements A_1, A_2, \dots, A_{r+1} in G such that

$$|A_1| \gg |A_2| \gg \dots \gg |A_{r+1}|$$

and such that no A_i is comparable to an element of \mathfrak{G}' . But then, since $\mathfrak{G}/\mathfrak{G}'$ is abelian, there would be $s > 0$ integers $e_1 \neq 0, e_2 \neq 0, \dots, e_s \neq 0$ such that

$$A = A_{i_1}^{e_1} A_{i_2}^{e_2} \dots A_{i_s}^{e_s} \in \mathfrak{G}'$$

²This theorem was conjectured by Professor Jennings.

where $i_1 < i_2 < \dots < i_r$. Let A_{i_1} belong to a C -class λ . Then A_{i_1} and A belong to \mathfrak{G}_λ , while

$$A_{i_1}^{e_1} \dots A_{i_r}^{e_r} \in G_\lambda, A_{i_1} \notin G_\lambda$$

Since G_λ/G_λ^* has no element of finite order, we have

$$A_{i_1}^{e_1} \notin G_\lambda.$$

However,

$$A \equiv A_{i_1}^{e_1} \pmod{G_\lambda}.$$

Hence $A \notin \mathfrak{G}_\lambda$. Therefore $A \in \lambda$, and A_{i_1} belongs to the same C -class λ as the element A in \mathfrak{G}' . But this contradicts our assumption that no A_i is comparable to an element in \mathfrak{G}' . Thus we have proved that \mathfrak{P} is a finite set, from which it follows easily that \mathfrak{G} is nilpotent.

Now suppose that \mathfrak{G} is an ordered, finitely generated, nilpotent group. Since \mathfrak{G} is ordered \mathfrak{G} is torsion-free. It has been proved by Jennings (4) that any finitely generated, torsion-free, nilpotent group satisfies the maximal condition for subgroups. Thus we know that the second part of Theorem 2 is also true.

Let \mathfrak{G} be an finitely generated, torsion-free, nilpotent group. It has been proved by Jennings (4) that such a group \mathfrak{G} has at least one central series

$$(1) \quad \mathfrak{G} = \mathfrak{F}_1 \supset \mathfrak{F}_2 \supset \dots \supset \mathfrak{F}_{k+1} = 1$$

with the properties

$$(2) \quad \mathfrak{F}_i/\mathfrak{F}_{i+1} \text{ is an infinite cyclic group, } i = 1, 2, \dots, k,$$

$$(3) \quad [F_i, G] \subseteq F_{i+1}.$$

Any central series (1) satisfying (2) and (3) is called an F -series of \mathfrak{G} . For an F -series of \mathfrak{G} let F_i be the representative in \mathfrak{G} of a generating element mod \mathfrak{F}_{i+1} ; then any element G of \mathfrak{G} may be written uniquely in the form

$$G = F_1^{e_1} F_2^{e_2} \dots F_k^{e_k}$$

where e_1, \dots, e_k are integers, positive, negative, or zero. The elements F_1, \dots, F_k are referred to as an F -basis for \mathfrak{G} . If we order elements G of \mathfrak{G} lexicographically with respect to e_1, \dots, e_k , then \mathfrak{G} becomes an ordered group. We shall say that this particular linear order of G is defined by the F -basis F_1, \dots, F_k .

Now let a finitely generated, torsion-free nilpotent group \mathfrak{G} be arbitrarily ordered. We have seen in the course of the proof of Theorem 2 that the set \mathfrak{P} for \mathfrak{G} is finite. Let \mathfrak{G}_λ of \mathfrak{G} be

$$(4) \quad \mathfrak{G} = \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \dots \supset \mathfrak{G}_k \supset 1.$$

It is clear that (4) is an F -series of G and that the linear order of \mathfrak{G} is defined by an F -basis associated with the F -series (4). Thus we have proved the following:

THEOREM 3. Every linear order of a finitely generated, torsion-free, nilpotent group \mathfrak{G} is defined by an F -basis of \mathfrak{G} .

4. In this section we shall show that an ordered, finitely generated, solvable group is not necessarily nilpotent by proving that $\mathfrak{F}/\mathfrak{F}''$ can be ordered, where \mathfrak{F} is an arbitrary free group with a finite (or countably infinite) number of generators and \mathfrak{F}'' is the second derived group of \mathfrak{F} .

Let the lower central series of commutator groups of $\mathfrak{G} = \mathfrak{F}/\mathfrak{F}''$ be

$$\mathfrak{G}_0 = \mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \dots,$$

where $\mathfrak{G}_1 = [\mathfrak{G}, \mathfrak{G}]$, $\mathfrak{G}_{n+1} = [\mathfrak{G}_n, \mathfrak{G}]$, $n = 1, 2, \dots$. K. T. Chen (1) has proved that the intersection of all \mathfrak{G}_n , $n = 1, 2, \dots$, is the unit element, and that every factor group $\mathfrak{G}_n/\mathfrak{G}_{n+1}$, $n = 0, 1, 2, \dots$, is a free abelian group.

Since $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ is a free abelian group, it can be ordered. After ordering every $\mathfrak{G}_n/\mathfrak{G}_{n+1}$ arbitrarily, we order \mathfrak{G} in the following way. Let $G = 1$ be any element in \mathfrak{G} . Then there exists an integer n such that $G \in \mathfrak{G}_n$, $G \notin \mathfrak{G}_{n+1}$. Let \bar{G} be the coset mod \mathfrak{G}_{n+1} represented by G . We set $G > 1$ if $\bar{G} > 1$, and $G < 1$ if $\bar{G} < 1$. For any two elements $G, H \in \mathfrak{G}$, we set $G > H$ if $GH^{-1} > 1$. It is easily seen that \mathfrak{G} is then a linearly ordered group.

It is also known (1) that $\mathfrak{G}_n \neq \mathfrak{G}_{n+1}$ for $n = 0, 1, 2, \dots$. Therefore \mathfrak{G} is not nilpotent.

The author wishes to express his gratitude to Professor S. A. Jennings for help and encouragement in the preparation of this paper.

REFERENCES

1. K. T. Chen, *Integration in free groups*, Ann. Math. (1), 54 (1951), 147-162.
2. K. A. Hirsch, *On infinite solvable groups*, Proc. Lond. Math. Soc. (2), Part I, 44 (1938), 53-60; Part II, 44 (1938), 336-344; Part III, 49 (1946), 184-194.
3. K. Iwasawa, *On linearly ordered groups*, J. Math. Soc. Japan, 1 (1948), 1-9.
4. S. A. Jennings, *The group ring of a class of infinite nilpotent groups*, forthcoming in Canadian J. Math.
5. A. G. Kurov and S. N. Cernikov, *Solvable and nilpotent groups*, Uspehi Math. Nauk (n.s.) 2 (1947), 18-59.
6. F. W. Levi, *Ordered groups*, Proc. Ind. Acad. Sci., 16 (1942), 256-263.

Dually Differentiable Points on Plane Arcs

PETER SCHERK, F.R.S.C.

Introduction. We consider a continuous one-parametric family A of line-elements in real projective plane. For one value of the parameter, A is supposed to be both differentiable and dually differentiable in a sense specified below. The structure of A near the corresponding line-element can then be described by means of a certain matrix. This yields a classification of these line-elements into 144 types. All of them are readily seen to exist.

1. An arc

 A :

$$P = P(t)$$

is the continuous image of an interval in the real projective plane. The images of different points are considered to be different points of A even when they coincide in the plane. We call A *open (closed)* if the parameter interval is open (closed). An *interior point* (the *left, right end-point*) of A is the image of an interior point (the left, right end-point) of the parameter interval.

Let $P(t_0)$ be a point of A . A *neighbourhood* N of $P(t_0)$ on A consists of the image points of a neighbourhood of t_0 on the parameter interval. If $P(t_0)$ is an interior point of A , N is given by

 N :

$$P = P(t)$$

$$t_l < t < t_r$$

where $t_l < t_0 < t_r$. It is decomposed by $P(t_0)$ into a *left neighbourhood* N_l and a *right neighbourhood* N_r corresponding to the parameter intervals $t_l < t < t_0$ and $t_0 < t < t_r$, respectively.

2. With each parameter t we associate a straight line $p(t)$ through $P(t)$ which depends continuously on t .

We call A (*right, left*) *differentiable* at $t = t_0$ if every straight line through $P(t_0)$ and $P(t)$ converges to $p(t_0)$ whenever t converges to t_0 (from the right, left). Similarly, A is called (*right, left*) *dually differentiable* at $t = t_0$ if $p(t_0) \cap p(t)$ converges to $P(t_0)$ whenever t converges to t_0 (from the right, left) ($t \neq t_0$).

A duality transforms the points $P(t)$ and *tangents* $p(t)$ of A into the tangents $p^*(t)$ and points $P^*(t)$ of an arc A^* . The relation between A and A^* is symmetric. The arc A is (*right, left*) differentiable at $t = t_0$ if and only if A^* is (*right, left*) dually differentiable there.

3. Let $P(t_0) \subset A$. We assume that $P(t_0)$ is not the right end-point of A and that A is both right differentiable and right dually differentiable at $t = t_0$. Choose any two straight lines g and h such that

$$(3.1) \quad P(t_0) \subset g, \quad g \neq p(t_0), \quad P(t_0) \not\subset h.$$

Then there is a right neighbourhood N_r of $P(t_0)$ such that

$$(3.2) \quad N_r \cap h \text{ and } N_r \cap g \text{ are void}$$

and that

$$(3.3) \quad g \cap h \not\subset p(t) \text{ and } h \cap p(t_0) \not\subset p(t) \text{ for every } P(t) \subset N_r.$$

The lines g and h divide the plane into two open half-planes. By (3.2), N_r lies entirely in one of them, the *right positive half-plane*. Its open complement is the *right negative half-plane*. The tangent $p(t_0)$ intersects the right positive (negative) half-plane in the *right positive (negative) half-tangent*

$$p_r^+ = p_r^+(t_0) \quad (p_r^- = p_r^-(t_0)).$$

The intersection of the straight line $P(t_0) P(t)$ with the right positive half-plane tends to p_r^+ if t converges to t_0 from the right.

In the same way, the two points $h \cap p(t_0)$ and $h \cap g$ divide h into two open segments. Since $p(t)$ is continuous, (3.3) implies that the intersections of the tangents of N_r with h lie entirely in one of them, the *right positive segment* h_r^+ . The other segment is the *right negative segment* h_r^- of h .

The right positive half-plane is divided by p_r^+ into two open quadrants. The *right positive (negative) quadrant* is adjacent to h_r^+ (h_r^-).

4. Put $e_r = 1$ ($e_r = 2$) if some N_r lies in the right positive (negative) quadrant. If every N_r meets p_r^+ , put $e_r = \infty$. Dually, define $e_r^* = 1$ ($e_r^* = 2$) if all the tangents of some N_r meet p_r^+ (p_r^-) and let $e_r^* = \infty$ if every N_r has tangents through $P(t_0)$.

These definitions seem to involve the entire projective plane. It should be noted however that the numbers e_r and e_r^* actually describe the local behaviour of A at the right of $t = t_0$. They are independent of the choice of g and h . If the numbers e_r, e_r^* are associated with A at $t = t_0$, then the pair e_r^*, e_r belongs to A^* there.

If a straight line meets both h_r^+ and the right negative quadrant, it will intersect p_r^+ . This holds true in particular of the tangents of N_r . Thus $e_r = 2$ ($e_r^* = 2$) implies $e_r^* = 1$ ($e_r = 1$). Hence only the following pairs e_r, e_r^* exist:

$$(4.1) \quad \begin{array}{c|c|c|c|c|c|c} e_r, e_r^* & 1, 1 & 1, 2 & 2, 1 & 1, \infty & \infty, 1 & \infty, \infty \\ \hline \text{Example} & D_1 & D_2 & D_2^* & D_3 & D_3^* & D_4 \end{array}.$$

5. We now define the examples of (4.1). Each of these arcs will be both differentiable and dually differentiable everywhere. In each case, we shall consider the left end-point O of the arc. We designate h as the line at infinity, while g and the tangent of the arc at O shall be the y - and x -axes of a rectangular cartesian coordinate system. The right positive half-plane will be given by $x > 0$. Thus p_r^+ is the positive x -axis. The interval h_r^+ of h will be the set of directions with positive slopes. We denote the quadrants by Roman numerals. Thus I is the right positive quadrant.

The arcs D_1, D_2, D_3 will lie in I , while D_4 intersects the positive x -axis in a sequence of points converging to O . The tangents of D_1 (D_2) intersect the positive (negative) x -axis, while those of any neighbourhood of O on D_3 or D_4 will intersect both the positive and the negative x -axes.

The dual D_2^* of D_2 lies in one quadrant of the right half-plane, say in IV . Then its tangents have positive slopes. They meet the positive x -axis.

D_3^* lies in the right half-plane. Any neighbourhood of O on D_3^* meets the positive x -axis infinitely often. The tangents of D_3^* meet the positive x -axis. We may assume that their slopes are positive.

5.1. D_1 is simply the arc

$$D_1: \quad y = x^2, \quad 0 \leq x < 1.$$

5.2. Construction of D_2 . Let

$$P_n = \left(\frac{1}{2^n}, \frac{1}{4^n} \right), \quad Q_n = \left(\frac{9}{2^{n+1}}, \frac{19}{3 \cdot 4^{n+1}} \right) \quad (n = 0, 1, 2, \dots).$$

By means of the segments

$$P_n Q_n: \quad y = f_{n,1}(x) = \frac{x}{6 \cdot 2^n} + \frac{5}{6 \cdot 4^n}, \quad \frac{1}{2^n} \leq x < \frac{9}{2^{n+1}},$$

and

$$Q_n P_{n+1}: \quad y = g_{n,1}(x) = \frac{x}{3 \cdot 2^n} + \frac{1}{3 \cdot 4^{n+1}}, \quad \frac{9}{2^{n+1}} \geq x > \frac{1}{2^{n+1}},$$

we first form the polygon $P_0 Q_0 P_1 Q_1 P_2 \dots$. Now put

$$f_{n,2}(x) = \frac{1}{33.49} \left(x - \frac{1}{2^n} \right) \left(x - \frac{9}{2^{n+1}} \right) (2^{n+6} x - 239),$$

$$g_{n,2}(x) = -\frac{1}{11.24} \left(x - \frac{1}{2^{n+1}} \right) \left(x - \frac{9}{2^{n+1}} \right) (2^{n+1} x - 5),$$

and replace each segment $P_n Q_n$ ($Q_n P_{n+1}$) by an arc

$$\alpha_n: \quad y = f_n(x) = f_{n,1}(x) + f_{n,2}(x), \quad \frac{1}{2^n} \leq x < \frac{9}{2^{n+1}},$$

$$\beta_n: \quad y = g_n(x) = g_{n,1}(x) + g_{n,2}(x), \quad \frac{9}{2^{n+1}} \geq x > \frac{1}{2^{n+1}},$$

with the end-points P_n and Q_n (Q_n and P_{n+1}). At P_n (at Q_n), α_n and β_{n-1} (β_n) have the same slope

$$\frac{6}{11 \cdot 2^n} \left(\frac{3}{11 \cdot 2^n} \right).$$

Thus the arc $\alpha_0 \beta_0 \alpha_1 \beta_1 \alpha_2 \dots$ is differentiable and dually differentiable everywhere.

The arc $\alpha_n(\beta_n)$ has exactly one inflection point. Its abscissa is

$$\frac{197}{2^{n+6}} \left(\frac{5}{2^{n+1}} \right).$$

Its slope there is equal to

$$\frac{23}{11 \cdot 2^{n+6}} \left(\frac{1}{11 \cdot 2^{n-2}} \right).$$

Thus the slope of $\alpha_n(\beta_n)$ is positive everywhere.

The tangent of the arc $\alpha_0\beta_0\alpha_1\beta_1\alpha_2\ldots$ at P_n (at Q_n) lies between P_nQ_n and P_nQ_{n-1} ($P_{n+1}Q_n$ and P_nQ_n). Hence it intersects the negative x -axis at a point which tends to O as $n \rightarrow \infty$. The same holds true of the tangents of the inflection points of α_n and β_n . This implies: Let a point P move through the arc $\alpha_0\beta_0\alpha_1\beta_1\alpha_2\ldots$. Then its tangent at P intersects the negative x -axis at a point converging to O . Thus the union D_2 of this arc with O has the required properties.

5.3. For D_3 we take Unger's arc (5)

$$D_3: \quad y = \begin{cases} x^2(3 + 2 \sin \ln x) & \text{if } 0 < x < 1 \\ 0 & \text{if } x = 0; \end{cases}$$

5.4. It remains to construct the arc D_4 . Put

$$P_n = \left(\frac{1}{2^n}, \frac{1}{4^n}\right), \quad Q_n = \left(\frac{1}{2^{n-1}}, \frac{2}{4^n}\right), \quad R_n = \left(\frac{1}{2^{n+2}}, \frac{-2}{4^{n+3}}\right) \quad (n = 1, 2, 3, \dots).$$

We now construct three families of parabolic arcs

$$\begin{aligned} \alpha_n: \quad y &= -\frac{1}{7} \left(2x^2 - \frac{13x}{2^n} + \frac{1}{4^{n-1}} \right), & \frac{1}{2^n} < x < \frac{1}{2^{n-1}}, \\ \beta_n: \quad y &= -\frac{1}{49} \left(\frac{25}{2} x^2 - \frac{85x}{2^n} + \frac{22}{4^n} \right), & \frac{1}{2^{n-1}} > x > \frac{1}{2^{n+2}}, \\ \gamma_n: \quad y &= -\frac{1}{14} \left(27x^2 - \frac{9x}{2^{n-2}} + \frac{31}{4^{n+1}} \right), & \frac{1}{2^{n+2}} < x < \frac{1}{2^{n+1}}. \end{aligned}$$

Thus $\alpha_n(\beta_n, \gamma_n)$ has the initial point $P_n(Q_n, R_n)$ and the end-point $Q_n(R_n, P_{n+1})$. Furthermore, α_n and β_n (β_n and γ_n , γ_n and α_{n+1}) have the same slopes

$$\frac{5}{7 \cdot 2^n} \text{ at } Q_n \left(\frac{45}{7 \cdot 2^{n+2}} \text{ at } R_n, \frac{9}{7 \cdot 2^{n+1}} \text{ at } P_{n+1} \right).$$

If a point moves on α_n from P_n to Q_n (on β_n from Q_n to R_n , on γ_n from R_n to P_{n+1}), the x -intercept of its tangent will vary monotonically from

$$\frac{1}{9 \cdot 2^{n-1}} \text{ to } \frac{-1}{5 \cdot 2^{n-2}} \left(\text{from } \frac{-1}{5 \cdot 2^{n-2}} \text{ to } \frac{97}{45 \cdot 2^{n+3}}, \text{ from } \frac{97}{45 \cdot 2^{n+3}} \text{ to } \frac{1}{9 \cdot 2^n} \right).$$

Thus the union D_4 of the arc $\alpha_1\beta_1\gamma_1\alpha_2\beta_2\gamma_2\alpha_3\ldots$ with the origin O has the required properties.

6. Let $P(t_0)$ be an arbitrary interior point of the arc A and let g be any straight line through $P(t_0)$. Then it can happen that there is a neighbourhood N of $P(t_0)$ such that $N_r \cap g$ and $N_l \cap g$ are void. Thus N_r and N_l are either separated by g or lie on the same side of g . In the first (second) case we say that g *intersects (supports)* A at $t = t_0$.

Suppose now that A is differentiable at $t = t_0$ and that $g \neq p(t_0)$. Then there is an N with the above property. If g intersects (supports) A at $t = t_0$, we put $a_0 = a_0(t_0) = 1$ ($a_0 = 2$). This definition is independent of the choice of g . It is equivalent to the following one: Let $Q \notin p(t_0)$. Choose an N such that the line through Q and a point $P(t) \in N$ passes through

$P(t_0)$ only if $t = t_0$. Then $a_0 = 1$ ($a_0 = 2$) if the set of these lines $QP(t)$ is (not) separated by $QP(t_0)$.

Define $a_1 = a_1(t_0) = \infty$ if $p(t_0)$ neither supports nor intersects. Otherwise, put $a_1 = 1$ or $a_1 = 2$ such that $a_0 + a_1$ is even (odd) if $p(t_0)$ supports (intersects). The pair (a_0, a_1) is called the *characteristic* of A at $t = t_0$ (2). It describes the behaviour of the points of A near $t = t_0$.

Suppose in addition that A is dually differentiable at $t = t_0$. Then the dual A^* of A is differentiable there and has a characteristic (a_0^*, a_1^*) which describes the behaviour of the tangents of A near $t = t_0$.

From the above, $a_0 = 1$ ($a_0^* = 1$) if and only if

$$p_r^+ \neq p_i^+ (h_r^+ \neq h_i^+).$$

If $a_1 = \infty$ ($a_1^* = \infty$), there are parameters $t \rightarrow t_0$, $t \neq t_0$ such that $P(t) \subset p(t_0)$ ($P(t_0) \subset p(t)$). Let N be sufficiently small. Then $a_1 = 1$ ($a_1 = 2$) if and only if the lines connecting $P(t_0)$ with the points of N_r and those through $P(t_0)$ and the points of N_l are separated by $p(t_0)$ (lie on the same side of $p(t_0)$; cf. (2)). Thus $a_1^* = 1$ ($a_1^* = 2$) if and only if the tangents of N_r and those of N_l meet distinct half-tangents (the same half-tangent) of $p(t_0)$.

7. Let $P(t_0)$ be a differentiable and dually differentiable interior point of the arc A . The preceding paragraph indicates the extent to which the structure of A at $t = t_0$ is described by the *first characteristic matrix*

$$(7.1) \quad \begin{pmatrix} a_0 & a_1 \\ a_0^* & a_1^* \end{pmatrix}.$$

It leads to a classification of the points $P(t_0)$ into $(2 \cdot 3)^2 = 36$ types.

A more detailed classification is given by the *second characteristic matrix*

$$(7.2) \quad \begin{pmatrix} e_l & a_0 & e_r \\ e_l^* & a_0^* & e_r^* \end{pmatrix}.$$

Here the pair e_l, e_l^* (e_r, e_r^*) describes the behaviour of A near and at the left (right) of $t = t_0$, while the numbers a_0, a_0^* determine the relative positions of the right and left positive quadrants. By §4 and §6, this yields $6 \cdot 2^3 \cdot 6 = 144$ types of points $P(t_0)$.

A change of orientation does not affect (7.1), while the outer columns of (7.2) have to be interchanged. A duality simply interchanges the rows of these matrices.

The connection between (7.1) and (7.2) is readily established. If e_r or e_l are infinite, then $a_1 = \infty$. Let both e_r and e_l be finite. Thus a_1 will be finite.

Choose N_r and N_l sufficiently small. Then the straight lines through $P(t_0)$ and the points of $N_r(N_l)$ will intersect h at points all of which lie in one of the two segments introduced in §3, say in $h_r(h_l)$. Thus $e_r = 1$ if $h_r = h_r^+$ and $e_r = 2$ if $h_r = h_r^-$. Similarly, $e_l = 1(2)$ if $h_l = h_l^+(h_l^-)$. Thus $e_r + e_l$ is even (odd) if h_r and h_l are right and left segments of h

with the same sign (with opposite signs). By §6, $a_0^* = 2(1)$ if $h_r^+ = h_l^+$ ($h_r^+ \neq h_l^+$). Hence $e_r + e_l + a_0^*$ is even (odd) if $h_r = h_l$ ($h_r \neq h_l$). Comparing this result with §6, we obtain

$$(7.3) \quad a_1 \equiv e_r + e_l + a_0^* \pmod{2}.$$

A duality yields

$$(7.4) \quad a_1^* \equiv e_r^* + e_l^* + a_0 \pmod{2}$$

if e_r^* and e_l^* are both finite.

By means of §§4 and 5 we can readily construct arcs with given characteristic matrices. The table (4.1) yields an arc $D_\lambda(D_\rho)$ associated with the pair e_l, e_l^* (e_r, e_r^*). Combining D_ρ with D_λ or with the reflection of D_λ with respect to one or both of the coordinate axes, we obtain a new arc with any prescribed pair a_0, a_0^* . This yields an example for every choice of the second characteristic matrix. Moreover, these examples are both differentiable and dually differentiable everywhere.

On account of (7.3) and (7.4), the above arcs also furnish examples for each of the first characteristic matrices.

REFERENCES

1. O. Delvendahl, *Die Singularitäten der Elementarkurven*, J. reine angew. Math., 182 (1940), 54-59.
2. P. Scherk, *Ueber differenzierbare Kurven und Bögen. I. Zum Begriff der Charakteristik*, Časopis pro pěst. mat. a fys., 66 (1937), 165-71.
3. —, *ibid. II. Elementarbogen und Kurve n-ter Ordnung im R_n* , Časopis pro pěst. mat. a fys., 66 (1937), 172-191.
4. G. Unger, *Maximalstetige Kurven, eine neue Charakterisierung der Kneser-Juelschen Bögen*, Elemente der Math., 8 (1953), 79-85.
5. —, *Ein Kriterium für die Kneser-Juelschen Kurven*, Arch. d. Math., 4 (1953), 143-153.

~~~~~

## Elementary Points on Plane Arcs

PETER SCHERK, F.R.S.C.

In this note, the characteristic matrices introduced in the preceding paper (=1) are connected with various order and differentiability properties. The work has been stimulated by two papers by Unger (4, 5 in 1) and some of the results may be considered refinements of the latter.

1. In the following,  $A$  denotes an arc in the sense of I, §1. It is supposed to be differentiable everywhere in the sense of I, §2. However, the continuity of its tangents  $p(t)$  is not required. Under these assumptions, every point  $P(t)$  of  $A$  still has a characteristic  $(a_0(t), a_1(t))$  with the properties of I, §6 (2).

The following remark is obvious.

LEMMA 1. *Let  $P(t)$  be an interior point of  $A$ . If a straight line through  $P(t)$  does not intersect  $A$  there (cf. I, §6), then it is either equal to  $p(t)$  or  $a_0(t) = 2$ .*

This lemma enables us to prove some projective generalizations of the Mean-Value Theorem.

LEMMA 2. *Let  $B$  denote the sub-arc of  $A$  determined by  $t_1 < t < t_2$ . Suppose the straight line  $g$  through the point  $Q$  passes through  $P(t_1)$  and  $P(t_2)$  and there is a straight line  $h$  through  $Q$  which does not meet  $B$ . Then there is a  $t'$  with  $t_1 < t' < t_2$  such that either  $Q \subset p(t')$  or  $a_0(t') = 2$ .*

*Suppose in addition that  $B \not\subset g$  but that a third point  $P(t_3)$  of  $B$  lies on  $g$ . Then there exists a  $t''$  with  $t_1 < t'' < t_2$  such that  $Q, P(t')$ , and  $P(t'')$  are not collinear and that either  $Q \subset p(t'')$  or  $a_0(t'') = 2$ .*

*Proof.* We may assume  $B \not\subset g$ . The set of straight lines through  $Q$  which meet  $B$  is closed and does not contain  $h$ . Thus this set contains two distinct extremal lines  $g'$  and  $g''$ . At least one of them, say  $g'$ , is different from  $g$ . It will have at least one point  $P(t')$  in common with  $B$ . Thus  $t_1 < t' < t_2$ . As  $g'$  cannot intersect  $B$  at  $t = t'$ , Lemma 1 yields the first part of our statement.

If  $g'' = g$ , then it does not intersect  $B$  at  $P(t_3)$ . Thus  $g''$  will yield a point  $P(t'')$  with the required properties whether  $g'' \neq g$  or not.

2. We call  $A$  *strongly differentiable* at  $t = t_0$  if every straight line through  $P(t)$  and  $P(t')$  converges to  $p(t_0)$  whenever  $t$  and  $t'$  tend to  $t_0$  ( $t \neq t'$ ). Part of the following observation should be known.

**THEOREM 1.** *Let  $P(t_0)$  be an interior (end-) point of  $A$ . Then  $A$  is strongly differentiable at  $t = t_0$  if and only if both  $p(t)$  is continuous at  $t = t_0$  and  $a_0(t) = 1$  for every  $t (\neq t_0)$  sufficiently close to  $t_0$ .*

*Proof.* Choose a straight line  $h$  such that  $P(t_0) \not\subset h$ . Making  $A$  smaller, we may assume that  $h$  and  $A$  are disjoint.

(i) Suppose  $A$  is not strongly differentiable at  $t = t_0$ . Then there is a sequence of straight lines  $g_n$  which meet  $A$  at two points  $P(t_{n,1})$  and  $P(t_{n,2})$  such that  $t_{n,1} < t_{n,2}$ ,  $t_{n,1} \rightarrow t_0$ ,  $t_{n,2} \rightarrow t_0$  but not  $g_n \rightarrow p(t_0)$ . We may assume  $g_n$  converges to a straight line  $g \neq p(t_0)$ .

By Lemma 2, there is to each  $n$  a parameter  $t'_n$  with  $t_{n,1} < t'_n < t_{n,2}$  such that either  $a_0(t'_n) = 2$  or  $g_n \cap h \subset p(t'_n)$ . With  $t_{n,1}$  and  $t_{n,2}$ ,  $t'_n$  will converge to  $t_0$ . Furthermore,  $g_n \cap h$  will converge to the point  $g \cap h$ . Thus  $p(t'_n)$  will converge to the straight line through  $P(t_0)$  and  $g \cap h$ , i.e. to  $g$ , unless  $a_0(t'_n) = 2$  for infinitely many indices  $n$ .

(ii) Suppose there is a sequence  $t_n \rightarrow t_0$  such that  $p(t_n)$  does not converge to  $p(t_0)$ . We may assume that  $p(t_n)$  converges to a straight line  $g \neq p(t_0)$ . The point  $Q_n = h \cap p(t_n)$  converges to  $Q = h \cap g$ .

Construct a sequence of neighbourhoods  $\nu_n$  of  $Q$  on  $h$  which converge to  $Q$  and such that  $Q_n \subset \nu_n$  for each  $n$ . Since  $A$  is differentiable at  $t_n$ , there is a  $t'_n \neq t_n$  converging with  $t_n$  to  $t_0$  and such that the line  $P(t_n)P(t'_n)$  meets  $\nu_n$ . This line will converge to the straight line through  $P(t_0)$  and  $Q$ , i.e., to  $g$ . Thus  $A$  is not strongly differentiable at  $t = t_0$ .

(iii) Suppose finally there is a sequence  $t_n \rightarrow t_0$  with  $a_0(t_n) = 2$ . Choose neighbourhoods  $N_n$  of  $P(t_0)$  on  $A$  which contain  $P(t_n)$  and shrink to  $P(t_0)$  as  $n \rightarrow \infty$ .

We may assume  $p(t_n) \rightarrow p(t_0)$ . Choose a point  $Q \not\subset p(t_0)$ . Then we may also assume that  $Q \not\subset p(t_n)$  for every  $n$ . Since  $a_0(t_n) = 2$ , the line  $P(t_n)Q$  supports  $N_n$  at  $P(t_n)$ . Hence there is a straight line through  $Q$  which meets  $N_n$  at least twice. It converges to  $P(t_0)Q$ . Again  $A$  cannot be strongly differentiable at  $t = t_0$ .

**3.** From now on let  $D$  denote an arc with continuous tangents which is both differentiable and dually differentiable everywhere. (The following example shows that the continuity of the tangents is not implied by the other assumptions. Put

$$\alpha_n: \quad y = (3 \cdot 2^{3n-1} - 2^{5n}x)x^2 + \frac{1}{2^{n+1}}, \quad 0 \leq x \leq \frac{1}{4n},$$

$$\beta_n: \quad y = 3(3 \cdot 2^{3n-2} - 2^{5n-1}x)x^2 + \frac{1}{2^{n+2}}, \quad \frac{1}{4n} \geq x \geq 0.$$

The union of  $O$  with the arc  $\alpha_0\beta_0\alpha_1\beta_1\alpha_2\dots$  is differentiable and dually differentiable everywhere but its tangent is not continuous at  $O$ .)

The proof of the following remark does not require the dual differentiability of  $D$  outside of  $P(t_0)$ .

**THEOREM 2.** Suppose  $P(t_0)$  is not the right end-point of  $D$ . Let  $a_0(t) = 1$  for all  $t > t_0$  sufficiently close to  $t_0$ . Then  $e_r = 1$  and  $e_r^* \neq 2$  (cf. I, §4).

*Proof.* Choose the lines  $g$  and  $h$  and the right neighbourhood  $N_r$  of  $P(t_0)$  according to I, §3. We may also assume  $a_0(t) = 1$  if  $P(t) \subset N_r$ .

Let  $P(t_1) \subset N_r$  and let  $Q$  denote the intersection of the straight line  $g_1 = P(t_0)P(t_1)$  with  $h$ . By the first part of Lemma 2, there is a  $t'$  with  $t_0 < t' < t_1$  such that  $Q \subset p(t')$ . In particular,  $Q \subset h_r^+$ . This holds for every  $t_1$ . Hence  $e_r = 1$ .

Since  $Q = g_1 \cap h_r^+ \neq p(t_0) \cap h$ , we have  $g_1 \neq p(t_0)$ . The lines  $g_1$  and  $h$  divide the plane into two half-planes. If  $t$  lies close enough to  $t_0$ ,  $t > t_0$ , then  $P(t)$  lies in the half-plane containing  $p_r^+$ . In particular, the line  $QP(t)$  will then intersect  $p_r^+$ . The proof of Lemma 2 then shows that  $t'$  can be chosen such that  $p(t') = QP(t')$  will also intersect  $p_r^+$ . Thus  $e_r^* \neq 2$ .

We now introduce a Condition  $\Gamma$  and its dual  $\Gamma^*$ .  $\Gamma(\Gamma^*)$ : If  $t$  is sufficiently close to  $t_0$ ,  $t \neq t_0$ , then

$$a_0(t) = 1 \quad (a_0^*(t) = 1).$$

**COROLLARY 1.** Suppose an interior point of  $D$  satisfies  $\Gamma$ . Then its first characteristic matrix has either the form

$$(3.1) \quad \begin{pmatrix} a_0 & a_0^* \\ a_0^* & a_0 \end{pmatrix} \text{ or } \begin{pmatrix} a_0 & a_0^* \\ a_0^* & \infty \end{pmatrix}.$$

If it also satisfies  $\Gamma^*$ , then its characteristic matrices are

$$(3.2) \quad \begin{pmatrix} a_0 & a_0^* \\ a_0^* & a_0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & a_0 \\ 1 & a_0^* \end{pmatrix} \quad (a_0, a_0^* = 1 \text{ or } 2).$$

*Proof.* By Theorem 2,  $\Gamma$  implies  $e_r = e_l = 1$  and  $e_r^*, e_l^* = 1$  or  $\infty$ . If  $e_r^*$  or  $e_l^*$  is infinite, then  $a_1^* = \infty$ . Otherwise  $a_1 \equiv a_0^* \pmod{2}$  and  $a_1^* \equiv a_0 \pmod{2}$ , i.e.  $a_1 = a_0^*$  and  $a_1^* = a_0$  (cf. I, §7).

If  $\Gamma^*$  holds too, then we apply Theorem 2 to the dual  $D^*$  of  $D$  obtaining  $e_r^* = e_l^* = 1$  and (3.2). This completes the proof.

The examples of I, 7 with  $\lambda = \rho = 1$  or 3 show that all these cases can actually occur.

Theorem 1 and Corollary 1 yield at once.

**COROLLARY 2.** The first characteristic matrix of a strongly differentiable interior point of  $D$  has the form

$$\begin{pmatrix} 1 & a_0^* \\ a_0^* & a_1^* \end{pmatrix} \quad (a_0^* = 1 \text{ or } 2; a_1^* = 1 \text{ or } \infty).$$

4. We call  $D$  maximally differentiable at  $t = t_0$  if both  $D$  and its dual  $D^*$  are strongly differentiable there. Obviously, the strong differentiability of  $D^*$  at  $t = t_0$  is equivalent to

$$(4.1) \quad \lim_{t, t' \rightarrow t_0} p(t) \cap p(t') = P(t_0) \quad (t \neq t').$$

Theorem 1 implies

**THEOREM 3.** *Let  $P(t_0)$  be an interior (end-) point of  $D$ . Then  $D$  is maximally differentiable at  $t = t_0$  if and only if  $a_0(t) = a_0^*(t) = 1$  for every  $t (\neq t_0)$  sufficiently close to  $t_0$ .*

**COROLLARY 3.** *The set of maximally differentiable points is open on  $D$ .*

*Proof.* By Theorem 3, a maximally differentiable interior (end-) point  $P(t_0)$  on  $D$  has a neighbourhood  $N$  such that  $a_0(t) = a_0^*(t) = 1$  for every  $P(t) \subset N$  (with  $t \neq t_0$ ). Let  $t_1 \subset N$ ,  $t_1 \neq t_0$ . Then  $N$  is also a neighbourhood of  $P(t_1)$ . By Theorem 3,  $D$  will be maximally differentiable at  $t = t_1$ .

By Theorem 3, a maximally differentiable point satisfies Conditions  $\Gamma$  and  $\Gamma^*$ . Thus this theorem and Corollary 1 yield

**COROLLARY 4.** *A maximally differentiable interior point of  $D$  has the characteristic matrices*

$$(4,2) \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Theorem 3 and its Corollary 4 imply the following result part of which is due to Unger (4, 5):

**COROLLARY 5.** *The following properties of  $D$  are equivalent:*

- (i) *It is maximally differentiable everywhere.*
- (ii)  *$a_0 = a_0^* = 1$  at every interior point of  $D$ .*
- (iii) *Every interior point of  $D$  has the characteristic matrices (4, 2).*

**5.** In this section we consider both arcs  $A$  and  $D$  (cf. §1 and §3).

The *order* of  $A$  is the least upper bound of the number of points which  $A$  has in common with any straight line. It may be infinite and is not less than two. The *order of a point* of  $A$  is the order of a sufficiently small neighbourhood. A point on  $A$  is called *elementary* if it has right and left neighbourhoods of order two.

The following remark is contained in (3).

**LEMMA 3.** *An arc  $A$  of order two is maximally differentiable everywhere.*

Our discussion will be based on this lemma and on

**THEOREM 4.** *Let  $D$  be maximally differentiable everywhere. Suppose there are a straight line  $h$  and a point  $H$  on  $h$  such that no point of  $D$  lies on  $h$  and no tangent of  $D$  passes through  $H$ . Then  $D$  has the order two.*

*Proof.* Suppose some straight line meets  $D$  in not less than three points. Let  $Q$  be its intersection with  $h$ . By Lemma 2 and Corollary 5, there are two interior points  $P(t')$  and  $P(t'')$  on  $D$  such that  $Q = p(t') \cap p(t'')$ . We now apply the first part of Lemma 2 to  $D^*$ . Thus there is a point  $P(t''')$  on  $D$  such that either  $P(t''') \subset h$  or  $a_0^*(t''') = 2$ . Either possibility has been excluded by our assumptions and by Corollary 5.

**COROLLARY 6.** *An arc  $D$  is maximally differentiable at those and only those points which have the order two.*

*Proof.* The sufficiency of this condition follows from Lemma 3.

Suppose conversely that a point of  $D$  is maximally differentiable. By Corollary 3, it has a neighbourhood  $N$  on  $D$  which is maximally differentiable everywhere. Making  $N$  sufficiently small, we may apply Theorem 4 to it. Thus  $N$  then has the order two.

We may call an arc  $A$  maximally differentiable at  $t = t_0$  if it is strongly differentiable there and (4, 1) holds true. If  $A$  is maximally differentiable everywhere, then its tangents are everywhere continuous (Theorem 1). Thus  $A$  then is an arc  $D$ . Combining this observation with Corollary 6 and Lemma 3, we obtain

**COROLLARY 7.** *The arc  $A$  is maximally differentiable everywhere if and only if each of its points has the order two.*

**REMARK.** Neither Corollary 6 nor Corollary 3 can be extended to arcs  $A$ . We obtain a counter-example by first replacing the parabola arc  $y = x^2$ ,  $1 \geq x \geq 0$ , by the polygon connecting its points  $(1/2^n, 1/4^n)$  and then rounding off its vertices. Put

$$\alpha_n: \quad y = \frac{3}{2^{n+1}}x - \frac{1}{2^{2n+1}}, \quad \frac{1}{11 \cdot 2^{n-3}} > x > \frac{7}{11 \cdot 2^n},$$

$$\beta_{n-1}: \quad y = \frac{11x^2}{8} - \frac{1}{2^{n+1}}x + \frac{5}{11 \cdot 2^{2n+1}}, \quad \frac{7}{11 \cdot 2^{n-1}} > x > \frac{1}{11 \cdot 2^{n-3}}.$$

Let  $A$  be the union of  $O$  with the arc  $\alpha_0\beta_0\alpha_1\beta_1\alpha_2 \dots$ . Then  $A$  is strongly differentiable everywhere and maximally differentiable at  $O$ . But the order of  $O$  is infinite and no neighbourhood of  $O$  is dually differentiable everywhere.

**COROLLARY 8.** *Given a point  $P(t_0)$  on an arc  $A$ . The following properties of  $P(t_0)$  are equivalent:*

- (i)  $P(t_0)$  is an elementary point.
- (ii) A neighbourhood of  $P(t_0)$  on  $A$  is an arc  $D$  and  $P(t_0)$  has the properties  $\Gamma$  and  $\Gamma^*$ .
- (iii) A neighbourhood of  $P(t_0)$  on  $A$  is an arc  $D$  and every point  $\neq P(t_0)$  of that neighbourhood has the characteristic matrices (4, 2).
- (iv) If  $t$  is sufficiently close to  $t_0$ ,  $t \neq t_0$ , then  $A$  is maximally differentiable at  $P(t)$ .

*Proof.* By Lemma 3, (iv) follows from (i). By Corollary 5, (iv) implies (iii). Obviously, (ii) is a consequence of (iii). Finally, (ii) and Corollary 5 imply that  $P(t_0)$  has right and left neighbourhoods which are maximally differentiable everywhere. Making them smaller, we may apply Theorem 4, obtaining (i).

It may be noted that the last corollaries combined with Corollary 1 imply the well known duality theorems for differentiable arcs of order two and for the characteristics of elementary points on plane differentiable arcs (cf. 1, 3).



PRINTED IN CANADA  
BY THE UNIVERSITY OF TORONTO PRESS

